

**ACTUALIZACIÓN DEL PLAN DE CONTINGENCIA, CONTROL DEL  
SOFTWARE INSTALADO, SOPORTE A USUARIOS Y ADMINISTRACION DE  
LA VIRTUALIZACION DE ESCRITORIOS EN LA EMPRESA UNE –  
TELEFÓNICA DE PEREIRA EN EL 2013**

**MELISSA CORREA RIOS**

**UNIVERSIDAD CATÓLICA DE PEREIRA  
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA  
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES  
PRÁCTICAS ACADÉMICAS  
PEREIRA  
2013**

**ACTUALIZACIÓN DEL PLAN DE CONTINGENCIA, CONTROL DEL  
SOFTWARE INSTALADO, SOPORTE A USUARIOS Y ADMINISTRACION DE  
LA VIRTUALIZACION DE ESCRITORIOS EN LA EMPRESA UNE –  
TELEFÓNICA DE PEREIRA EN EL 2013**

**MELISSA CORREA RÍOS**

**INFORME DE PRÁCTICA ACADÉMICA**

**TUTOR  
INGENIERO ALVARO MORALES**

**UNIVERSIDAD CATÓLICA DE PEREIRA  
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA  
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES  
PRÁCTICAS ACADÉMICAS  
PEREIRA  
2013**

## TABLA DE CONTENIDO

INTRODUCCION .....	10
1. PRESENTACIÓN DE LA ORGANIZACIÓN .....	11
1.1. HISTORIA .....	11
1.1.1 El montaje .....	11
1.1.2 La financiación .....	11
1.1.3 Hechos históricos .....	12
1.2. MISIÓN .....	14
1.3. VISIÓN .....	14
1.4. VALORES .....	14
1.5. POLITICA DEL SGI DE UNE-TELEFONICA DE PRERIRA S.A.....	15
1.6. SERVICIOS QUE PRESTA .....	15
1.6.1 Voz.....	16
1.6.2 Conectividad .....	16
1.6.3 Internet.....	16
1.6.4 Servicios profesionales .....	16
1.6.5 Data center.....	16
1.6.6 Entretenimiento .....	17
1.7. ESTRUCTURA ORGÁNICA .....	17
2. DIAGNÓSTICO DEL ÁREA DE INTERVENCIÓN O IDENTIFICACIÓN DE NECESIDADES.....	20

3. EJE DE INTERVENCION.....	21
3.1. PLAN DE CONTINGENCIA .....	21
3.2. FUNCIONES:.....	21
4. JUSTIFICACION DEL EJE DE INTERVENCION.....	23
5. OBJETIVOS .....	24
5.1 OBJETIVO GENERAL .....	24
5.2 OBJETIVOS ESPECIFICOS .....	24
6. MARCO TEORICO .....	25
6.1 ¿QUE ES UN PLAN DE CONTINGENCIA? .....	25
6.2 PLAN DE CONTINGENCIA EN EL ÁREA DE TI. ....	25
6.3 ETAPAS PARA ELABORAR UN PLAN DE CONTINGENCIA EN EL ÁREA DE TI.....	26
6.3.1 Análisis y valoración de Riesgos.....	26
6.3.2 Jerarquización de las aplicaciones:.....	26
6.3.3 Establecimiento de requerimientos de recuperación:.....	27
6.3.4 Ejecución:.....	27
6.3.5 Pruebas y simulaciones: .....	27
6.3.6 Documentación: .....	28
6.3.7 Difusión y mantenimiento .....	28
6.4 PLANES DE RESPALDO .....	29
6.4.1 Respaldo interno: .....	29
6.4.2 Respaldo externo: .....	29
6.5 TIPOS DE CONTINGENCIA DE ACUERDO A LOS DAÑOS SUFRIDOS ..	29

6.6 TIPOS DE CONTINGENCIAS DE ACUERDO AL GRADO DE AFECTACIÓN .....	30
6.7 GRUPO DE TRABAJO Y DEFINICIÓN DE ROLES PARA LA PREPARACIÓN DEL PLAN DE CONTINGENCIA .....	30
6.7.1 Presidente del Grupo de Trabajo: .....	30
6.7.2 Coordinador General: .....	31
6.7.3 Coordinador de Redes y Comunicaciones: .....	31
6.7.4 Coordinador de Soporte Técnico: .....	32
6.7.5 Coordinador de Sistemas: .....	32
7. CRONOGRAMA DE ACTIVIDADES .....	33
8. PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS .....	34
8.1 PLANIFICACIÓN Y DISEÑO DEL PLAN PREVENTIVO Y REACTIVO .....	34
8.1.1 Formatos plan de contingencia .....	36
8.2 AUDITORÍA ESTADO DE EJECUCIÓN DE BACKUPS .....	38
8.2.1 Backup vRanger: .....	38
8.2.2 Backup Directorios NAS y freeNAS: .....	40
8.2.3 Backup TSM: .....	42
8.3 CONTROL DE SOFTWARE CON ARANDA SOFTWARE METRIX® .....	43
8.4 OWNCLOUD .....	45
8.5 VIRTUALIZACIÓN DE ESCRITORIOS .....	47
8.5.1 Thin Client .....	48
8.5.2 VMware vSphere Client .....	50
8.5.3 Agregar un nuevo usuario al entorno virtual. ....	51

8.5.4 Herramientas de administración de la virtualización de escritorios. ....	55
9. CONCLUSIONES .....	68
10. RECOMENDACIONES .....	70
11. BIBLIOGRAFIA .....	71

## TABLA DE ILUSTRACIONES

GRÁFICO 1. Organigrama de la empresa. ....	18
GRÁFICO 2. Organigrama de la Subgerencia de TI. ....	19
GRÁFICO 3. Cronograma de actividades. ....	33
GRÁFICO 4. Página de documentación switches. ....	35
GRÁFICO 5. Página de documentación servidores. ....	35
GRÁFICO 6. Documentación almacenada en Tortoise SVN (aplicación para el control de versiones). ....	36
GRÁFICO 7. Formato Plan de recuperación de Backups. ....	37
GRÁFICO 8. Formato pruebas plan de contingencia. ....	38
GRÁFICO 9. Correo vRanger. ....	39
Grafico 10. Bitácora backups vRanger. ....	40
GRÁFICO 11. Correo directorios NAS. ....	41
GRÁFICO 12. Bitácora repositorio NAS. ....	41
GRÁFICO 13. Informe backup TSM. ....	42
GRÁFICO 14. Bitácora backups TSM. ....	43
GRÁFICO 15. Control de licenciamiento por aplicación. ....	44
GRÁFICO 16. Clasificación del software en Aranda Software Metrix. ....	45
GRÁFICO 17. OwnCloud logueo administrador. ....	46
GRÁFICO 18. OwnCloud Administración de la página. ....	47
GRÁFICO 19. Equipo trabajando con la tecnología PColP. ....	47
GRÁFICO 20. Dell Wyse P20 Zero Client. ....	48
GRÁFICO 21. Inventario de Thin Client instaladas por sede. ....	49
GRÁFICO 22. Entrono de administración de virtualización VMware vSphere Client. ....	50
GRÁFICO 23. Adición a grupo Thin Client. ....	52
GRÁFICO 24. Carpetas personales o backup. ....	53
GRÁFICO 25. Registro a Consola Sentry. ....	54

GRÁFICO 26. Agregar Entitlement. ....	55
GRÁFICO 27. Ventana de logueo a VMware View Administrator. ....	56
GRÁFICO 28. Entorno de administración VMware View. ....	57
GRÁFICO 29. Pools. ....	58
GRÁFICO 30. Función Reset. ....	59
GRÁFICO 31. Función recompouse. ....	60
GRÁFICO 32. Asignar usuario a una máquina específica. ....	61
GRÁFICO 33. Entitlement. ....	62
GRÁFICO 34. Consola web para administración de PCoIP. ....	63
GRÁFICO 35. Escaneo de Dispositivos Thin client. ....	64
GRÁFICO 36. Agregar grupo nuevo. ....	65
GRÁFICO 37. Asignación de maquina a un grupo. ....	65
GRÁFICO 38. Actualización Firmware. ....	66
GRÁFICO 39. Versión firmware 4.0.2. ....	67



## SÍNTESIS

SÍNTESIS
<p>Este trabajo consiste en la planeación y ejecución del plan de contingencia realizado cada seis meses en la empresa UNE-telefonica de Pereira en donde se llevaran a cabo una serie de procedimientos para demostrar y siendo el caso mejorar la efectividad de los diferentes servidores, recuperando datos imprescindibles dentro de la empresa a la hora de que ocurra cualquier hecho inesperado con respecto a todos los datos e información que se encuentran allí almacenados.</p> <p><b>Descriptores:</b> Plan de contingencia, datos, servidores.</p>

ABSTRACT
<p>This work involves the planning and execution of contingency plan made every six months in the UNE-Telefonica de Pereira company where carried out a series of procedures to demonstrate and to be the case to improve the effectiveness of different servers, retrieving data essential within the company when any unexpected event occurs with respect to all data and information that are stored there.</p> <p><b>Descriptors:</b> Contingency Plan, data servers.</p>

## INTRODUCCION

El presente trabajo se refiere al tema propuesto para el desarrollo de la práctica profesional en donde se acordó llevar a cabo un plan de contingencia, el cual se refiere al conjunto de medidas encaminadas a restaurar el funcionamiento normal de una actividad tras la alteración producida por un accidente; en este caso de un accidente con la infraestructura informática de la empresa UNE-Telefónica de Pereira.

Este trabajo se desarrollara con el fin de tener un control de la infraestructura y la información que en ella se encuentra corroborando que si sea funcional a la hora de que un hecho inesperado ocurra y enfocado en el interés académico debido a que aporta conocimiento al ir teniendo práctica y la experiencia de cómo funcionan los equipos de la parte de infraestructura en su interior y exterior y hacer practica de ello se tendrá previo conocimiento de que es, como funciona y para qué sirve y además es de interés profesional debido a que la empresa tiene que estar siempre preparada para cualquier tipo de accidentes que puedan ocurrir y de esta manera poder tomar medidas en el asunto a la hora de enfrentarlas cuando se presenten realmente.

Para este procedimiento se planea primero que todo evaluar a que servidores no se les ha hecho plan de contingencia últimamente y así conocer el estado de los servidores a los que sea necesario hacerle prueba de contingencia dentro de la empresa para luego llevar a cabo un esbozo o diseño del plan a seguir para evaluar el debido y correcto funcionamiento de los servidores tal y como se planeó que se estuvieran ejecutando sus correspondientes funciones desde el momento que fueron montados, luego ver si es viable realizar dichas pruebas, ya que se tiene mucho en juego; además de que los usuarios de la empresa diariamente están trabajando en ellos y por ultimo ejecutar dicho plan para sacar conclusiones y mejorar algunos servicios si es el caso.

## **1. PRESENTACIÓN DE LA ORGANIZACIÓN**

### **1.1. HISTORIA**

Un grupo de visionarios Pereiranos viajó a Alemania en 1925 a la Feria de la Ciencia y se dio cuenta de que las plantas de teléfonos existentes en Bogotá, Cali y Medellín serían obsoletas en poco tiempo. Necesitaban para su operación de telefonistas e interconexión de cables en cada llamada. Decidieron que para Pereira había que comprar una planta automática. Corría el año de 1927 cuando se firmó el contrato directamente entre el Concejo Municipal que presidía Julio Castro y la empresa alemana Siemens. Un hito histórico para la ciudad y el continente, pues hasta ese momento, sólo Montevideo, la capital uruguaya, contaba con telefonía automatizada.

En ese mismo año (1927), llegaron a la Pereira de calles empedradas tiradas a cordel y por las que transitaban recuas de mulas con su abundante carga, provenientes desde todas las direcciones, y construcciones de una o dos plantas, 3 técnicos alemanes de la Siemens: Alejandro Clark, Miguel Mauser y Enrique Hoppe.

El trío alemán inició sus labores utilizando personal colombiano, sin ninguna capacitación. Fue así como se formaron los tres más importantes personajes del servicio telefónico de aquella primera época: Luis Angel Piedrahita, Juan de J. Franco y Florentino Arias.

#### **1.1.1 El montaje**

Se inició el montaje de la primera planta telefónica automática de Colombia, con la orientación y el control de todos los trabajos del ingeniero Alejandro Clark, seguido por Misael Mausser, responsable del montaje de planta y Enrique Hoppe como empalmador de cables. Los 3 eran maestros del personal colombiano, pero además en un cruce fraterno, aprendieron de éstos las bondades de la tierra del café.

#### **1.1.2 La financiación**

La financiación para una ciudad apenas en formación, de tan solo un poco más de 50 años de fundada, significó un gran esfuerzo de sus gentes y un empréstito del Banco Central Hipotecario en cuantía de un millón de pesos del cual se tomaron \$120 mil pesos para el nuevo servicio de teléfonos. Mediante el acuerdo No.50 de septiembre 30 de 1927 el Concejo Municipal de Pereira aprobó el contrato con Siemens y Halke " para dar servicio a mil líneas automáticas, con todo su equipo

de comunicación que permita posteriormente su fácil aumento hasta 10.000 líneas sin que haya necesidad de modificación de ninguna clase".

#### PEREIRA EN 1929 YA TENIA TELEFONIA AUTOMATICA

La población de Pereira para el año de 1929 era apenas de 55 mil habitantes de pie descalzo y actividades primarias de sustento diario, con los parques de La Libertad, El Lago y la Plaza de Bolívar como sus límites y las aguas aún limpias y abundantes del río Otún como su frontera. Para este contexto histórico la celebración de la inauguración de su planta telefónica era desconcertante, casi innecesaria, pero señalaba características propias de los pereiranos y que la historia se ha encargado de reconocerles: tenacidad y empuje. Buscar teléfonos automáticos en semejante latitud y condiciones no era más que la premonición de grandes obras del futuro y una confianza de que el teléfono formaría parte sustancial de una vida moderna muy cerca a los aleros de sus casas de tapia, pesebrera y grandes patios llenos de flores.

El primer Gerente fue don Manuel Orozco Patiño.

La primera campaña de mercadeo, fue la instalación de dos teléfonos de servicio público gratuitos en el más importante establecimiento de la época: el café Centro Social en la 18 con 8a. El objeto de la campaña era ganar suscriptores "El teléfono es un magnífico compañero. Entonces si todo el mundo tiene, usted porqué carece de él", rezaba la frase de combate de esa campaña.

#### 1.1.3 Hechos históricos

1934 Se dio servicio a la región, hoy municipio, de Dosquebradas. Se estableció la larga distancia, por cable físico, con Santa Rosa de Cabal, Chinchiná y Manizales. En 1935 Se extendió el servicio a la ciudad de Cartago.

1966 se hicieron ensanches a 5 mil líneas más, lo que condujo a incrementar la numeración de 4 a 5 números, lo que además llevó a implementar una nueva central de mil líneas mediante el traslado de los correspondientes equipos a la sub central de Dosquebradas.

1996 Con el proceso de instalación de las 80 mil líneas, se marca otro hito histórico de la Empresa y la ciudad. Se satisfizo la demanda de varios años. Cualquier Pereirano podía ahora tener su propia línea telefónica.

En el año de 1996 mediante el acuerdo No. 30 expedido por el Concejo Municipal de Pereira en el que se facultaba al Alcalde Juan Manuel Arango Vélez, para la transformación de una de las organizaciones más importantes de la ciudad y la región en proceso de liquidación, Las Empresas Públicas de Pereira, como

aparece en los documentos de la época:

Acuerdo No 30/96 “Por el cual se autoriza al alcalde de Pereira para transformar el establecimiento público “empresas públicas de Pereira” en sociedades por acciones y se dictan otras disposiciones”.

Así quedan conformadas las empresas prestadoras de los servicios públicos:

- Empresa de energía de Pereira S.A. E.S.P.
- Empresa de acueducto y alcantarillado de Pereira S.A. E.S.P
- Empresa de telecomunicaciones de Pereira S.A. E.S.P.
- Empresa de aseo de Pereira S.A. E.S.P.
- Empresa multiservicios S.A.

Hasta el año 2006 las Empresas Públicas de Medellín ha adquirido más del 56% de la participación accionaria de la compañía, e introdujo nuevos servicios no sólo de redes telefónicas e Internet, sino un nuevo canal de televisión gracias al servicio por suscripción. A pesar que sus acciones corresponden en más de la mitad a la empresa antioqueña, la Empresa sigue teniendo autonomía en las decisiones para la prestación de los servicios en el Área Metropolitana del Centro Occidente, Santa Rosa de Cabal y Cartago; el 43% de las acciones pertenecen al Municipio de Pereira, y el otro 0.14% pertenece a los ex trabajadores y jubilados.

El estar a la vanguardia de la innovación en tecnología, en los procesos de gestión interna, en el cumplimiento de estándares internacionales de calidad y gestión social a Telefónica de Pereira, obtener en los últimos años certificaciones ISO 9001(certificado de calidad) y de adhirió al Pacto Mundial de la ONU. En el año 2003 UNE Telefónica de Pereira logró su certificación ISO 9001 conferida por la firma francesa BVQI.

En el 2005 la Empresa se adhirió al Pacto Mundial de las Naciones Unidas, para el respeto no sólo de los derechos laborales, humanos, sino también medioambientales, y de lucha contra la corrupción. Hoy día, el documento continúa siendo objeto de sensibilización a los trabajadores, a través de los medios internos, con el fin de informar a sus clientes internos y externos el documento que los hizo integrantes a dicho Pacto de la ONU. El 25 de noviembre del mismo año, Telefónica logró su certificación en OHSAS 18001 contando como ente certificador a la misma de la firma francesa BVQI, con lo cual se convierte en

la primera empresa de Servicios en Telecomunicaciones en Colombia certificada contra esta norma.

En 2006 la Empresa inicia su proceso de verificación de requisitos para certificación en los sistemas de Gestión Ambiental con la norma 14000 y el de Responsabilidad Social (norma S.A. 8000) convirtiéndose en la primera empresa a nivel nacional en lograr certificar estos cuatros sistemas de gestión e implementar uno de forma Integral.

A finales del año 2007 se empezó hacer el cambio de sede para el Edificio Inteligente, donde se encuentran hoy en día las instalaciones de UNE- Telefónica de Pereira y donde se están llevando proyectos de alta exigencia y mejoramiento como Proyecto Evolución, el cual se ejecutó con el acompañamiento de la firma consultora BM Consulting Group, buscando incrementar la productividad dentro de la Empresa, fundamentado en 5 ejes específicos: 1. Mejora en los tiempos de las operaciones 2. Mejora en los procesos de la fuerza comercial. 3. Incremento de la productividad administrativa. 4. Optimización de gastos. 5. Incorporación de habilidades gerenciales.

Actualmente cuenta con una excelente oferta de productos de telecomunicaciones, empaquetamientos y calidad en la prestación de servicios; es una empresa 100% nacional, con un espectacular equipo de trabajo, hacemos la diferencia con talento humano.

## 1.2. MISIÓN

Nos dedicamos a entregar soluciones integrales de información y comunicaciones enfocadas en el cliente en forma efectiva.

## 1.3. VISIÓN

Al 2013 lograremos un crecimiento por línea de negocio por encima del presentado en el país, manteniendo el margen EBITDA por cada una de ellas, con responsabilidad social empresarial.

## 1.4. VALORES

- Foco en el Cliente:  
Existimos para comprender, anticipar y responder de manera memorable a las necesidades de nuestros clientes.

- **Orientación a Resultados:**  
Nuestros objetivos son claros y retadores pero alcanzables y medibles.
- **Innovación:**  
Empleamos nuestra creatividad para satisfacer de la mejor manera las necesidades de nuestros clientes y resolver efectivamente sus problemas.
- **Agilidad:**  
Nos esforzamos por adaptar nuestros procesos cuando se trata de responder a las necesidades de nuestros clientes y el mercado.
- **Trabajo en Equipo:**  
Contamos con objetivos comunes y participamos proactiva, respetuosa y armónicamente en lograrlos.
- **Responsabilidad Social Empresarial:**  
Estamos convencidos de nuestra responsabilidad por el mejoramiento social y económico de la comunidad a la que servimos y participamos activamente en su sostenibilidad y progreso.

#### 1.5. POLITICA DEL SGI DE UNE-TELEFONICA DE PRERIRA S.A

“El éxito de la Empresa en los servicios de TIC’s, depende de la satisfacción de las necesidades y expectativas de sus clientes; promoviendo y conservando ambientes de trabajo seguros y la salud de las personas que intervienen en sus procesos, propiciando la protección ambiental y la prevención de la contaminación a través del afianzamiento de una comunicación que propenda por el fortalecimiento de la cultura ambiental de los grupos de interés pertinentes, basada en relaciones de respeto y confianza mutua, en cumplimiento de las disposiciones vigentes, los compromisos voluntarios suscritos en el ámbito de su actuación y de la norma SA 8000, con un permanente compromiso de efectividad y de mejoramiento continuo”.

#### 1.6. SERVICIOS QUE PRESTA

En la actualidad UNE EPM Telecomunicaciones S.A. tiene una importante participación accionaria en las empresas Colombia Móvil (25%), EPM Bogotá (66.46%), Empresa de Telecomunicaciones de Pereira (56%) y Edatel (56%).

Gracias a estas integraciones y participaciones hoy UNE ofrece más y mejores servicios a precios competitivos. Ofertas comerciales empaquetadas que se

ajustan a la necesidad y a los gustos de los hogares, las personas y las empresas.

Hoy, UNE cuenta con un portafolio de servicios que incluye:

#### 1.6.1 Voz

- Telefonía Fija: Citofonía Virtual, PBX, RDSI, Marcación Directa, Línea 113, Troncal Ordinaria
- Telefonía IP: VozIP, Conmutador Virtual, Voz Administrada
- Red Inteligente: Líneas 800, Número Único, Líneas 901, Telecontenidos, Teleconferencia
- Larga Distancia Nacional e Internacional
- Telefonía Pública
- Telefonía Móvil
- Tarjetas prepago

#### 1.6.2 Conectividad

- Lan to Lan
- VPN
- Portador
- Multilan

#### 1.6.3 Internet

- Banda Ancha: XDSL, WinFax
- Dedicado: Internet Empresarial
- Conmutado

#### 1.6.4 Servicios profesionales

- Mesa de Ayuda
- Soluciones Integradas

#### 1.6.5 Data center

- Alojamiento de Equipos
- Hastings Dedicado
- Web Hastings
- Hosting de Base de Datos
- Mail Hosting
- Disco Duro Virtual
- ASP
- SchollWeb
- WebComercio



#### 1.6.6 Entretenimiento

- Televisión por Suscripción, incluido el servicio Pague por Ver (PPV)
- Televisión Interactiva
- Televisión Digital Interactiva en Alta Definición
- Servicios de Valor Agregado
- Datos
- Videoconferencia

Estos servicios están soportados con múltiples tecnologías de redes y de accesos, en las que siempre UNE ha estado a la vanguardia, tales como TDM, HFC, FR/ATM, FO, ADSL, WiFi, WiMAX.

#### 1.7. ESTRUCTURA ORGÁNICA

La estructura orgánica de la empresa se compone de las siguientes áreas:

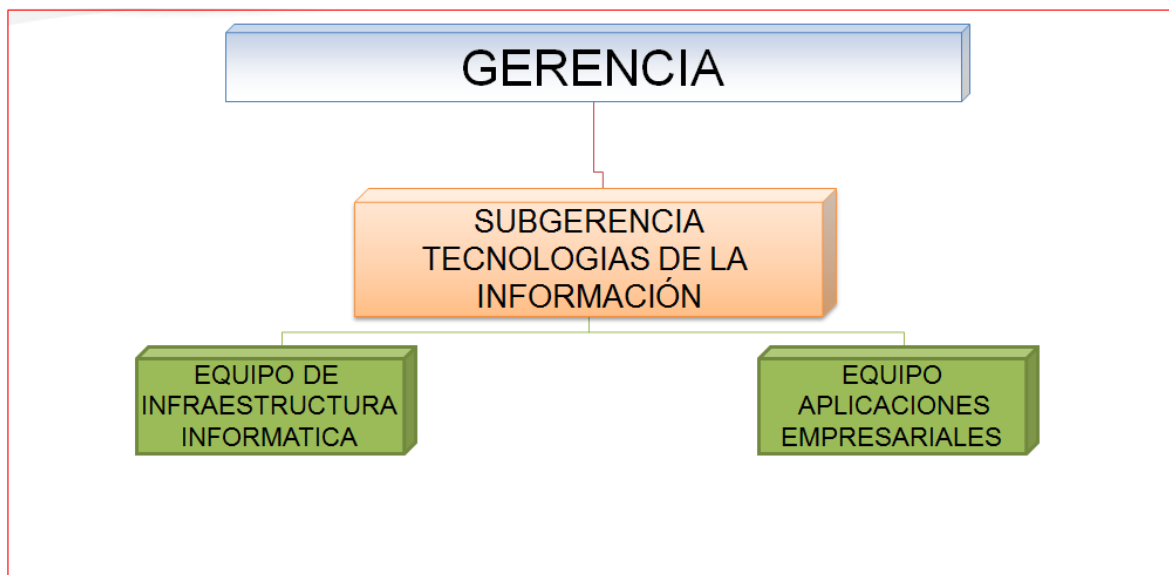
- gerencia
- dirección de control interno
- secretaria general
- subgerencia de servicio al cliente
- subgerencia de hogares y personas
- subgerencia de negocios empresariales
- subgerencia técnica
- subgerencia de administración y finanzas
- subgerencia de tecnologías de la información
- subgerencia de gestión humana y calidad

[illegible]

La subgerencia de tecnologías de la información, está conformada por dos equipos de trabajo:

- 18

**GRÁFICO 2. Organigrama de la Subgerencia de TI.**



Fuente: Intranet de la empresa

## **2. DIAGNÓSTICO DEL ÁREA DE INTERVENCIÓN O IDENTIFICACIÓN DE NECESIDADES**

La necesidad fundamental que se requiere abordar con la práctica es la relacionada con los backup que realizan los servidores de la empresa verificando que su ejecución sea exitosa y de no ser así dar el reporte de lo sucedido a las personas indicadas de solucionar el problemas además de dejar registrado cualquier novedad en la bitácoras debido a que cada año se realizan unas auditorías realizadas por la PricewaterhouseCoopers.

Además de hacer un apoyo en cuanto a la categorización y verificación del software instalado en la empresa por medio del software Aranda Metrix ya que con este aporte la empresa se va a ver beneficiada en cuanto al cumplimiento de normatividades pues la que la empresa se hace responsable del software que hay instalado en los equipos, debido a que no debe haber software sin licencia instalado en ningún computador de la empresa, ya que esto violaría los derechos de autor y la empresa se vería obligada a pagar una multa millonaria por los llamados gaps.

También la empresa debe estar preparada para una situación de riesgo en la cual se puede llegar a ver afectada la información que esta almacenada en los servidores, es por esto que se debe tener un plan de contingencia para así estar preparado en el momento en que sea requerido recuperar la información.

### 3. EJE DE INTERVENCION

#### 3.1. PLAN DE CONTINGENCIA

El eje de intervención está enfocado en el equipo de infraestructura de la empresa y el control de la información contenida en ella, en donde se intervendrá de la siguiente manera:

Por seguridad de la empresa se debe establecer un procedimiento formal y por escrito que indique las acciones a seguir frente a determinados y probables riesgos verificando el debido funcionamiento de la infraestructura y todas sus conexiones para la eficiente ejecución de sus continuos procesos al interior de la empresa UNE-telefónica de Pereira.

Documentación actualizada de toda la información de los servidores actuales de la empresa, con el fin de tener un listado de pasos a seguir para recuperar la información de las diferentes backup en caso de una emergencia.

Generar diagramas de los servidores en las que se identifiquen las conexiones de UTP y fibra óptica.

Custodiar la Información empresarial siguiendo procesos de definición de backup, mantenimiento de los backup existentes y revisión de la elaboración efectiva de dichos backup.

Ejecutar los procedimientos que se hicieron de manera escrita en el plan de contingencia, documentando lo evidenciado para control y mejoramiento de los riesgos obtenidos.

#### 3.2. FUNCIONES:

- **Auditoria:** Estar pendiente de los backup vRanger, freenas, BDs, tsm y backups externos documentando los éxitos o fracasos de su ejecución; además de los usuarios que se han retirado de la empresa para desactivación de permisos y roles dentro de la organización.
- **Owncloud:** instalar y ejecutar un software de servidor en la nube de manera privada para el almacenamiento de información en la empresa a través de la web.
- **Vmware view:** Manejo de toda la herramienta VMware view client para dar soluciones automatizadas y seguras a todos los equipos y usuarios de Une

telefónica de Pereira además de brindar acompañamiento a los empleados para dar soporte cuando sea necesario.

- **Control de Software:** controlar el software existente en la empresa por medio de la plataforma Aranda Software Metrix, clasificando el software de la empresa por grupos entre permitidos y no permitidos. Colaborar con el control de software haciendo uso de esta herramienta, generando las alarmas del caso además de realizar control de licencias.
- **Soporte:** Brindar soporte a usuarios en momentos en que sea requerido (implementaciones o soportes masivos).
- **Documentación:** Colaborar con la documentación de TI referida tanto a esquemas implementados en sus servidores, como a procedimientos del área.
- **Outsourcing de impresión con TES:** verificar y supervisar la ejecución y el cumplimiento de las obligaciones del contrato con TES LTDA (Tecnología Equipos y Suministros) encargada de dar soporte a las impresoras de la empresa y elaborar una bitácora mensual para el control de la cantidad de impresiones realizadas por mes en cada impresora.

#### **4. JUSTIFICACION DEL EJE DE INTERVENCION**

El objetivo principal de diseñar y ejecutar un Plan de Contingencias, es poder prevenir y controlar sucesos no planificados, pero previsibles, y describir la capacidad y las actividades de respuesta inmediata para controlar las emergencias de manera oportuna, eficaz y de esta forma no tener pérdidas masivas de información que son imprescindible para el continuo desenvolvimiento de la empresa.

## **5. OBJETIVOS**

### **5.1 OBJETIVO GENERAL**

Diseñar y ejecutar el plan de contingencia (plan preventivo y reactivo) para el área de infraestructura de UNE-Telefónica de Pereira, con el fin de estar preparados ante una situación de emergencia, minimizando consecuencias negativas en su infraestructura y la información contenida en ella.

### **5.2 OBJETIVOS ESPECIFICOS**

- Planificar y diseñar el plan preventivo y reactivo.
- Realizar pruebas de viabilidad del plan de contingencia.
- Ejecutar el plan de contingencia.
- Proceder con la recuperación de los datos obtenidos al elaborar el plan de contingencia.
- Determinar las conclusiones y posibles mejoras según datos arrojados en la ejecución del plan de contingencia.



## **6. MARCO TEORICO**

### **6.1 ¿QUE ES UN PLAN DE CONTINGENCIA?**

Un plan de contingencia es un tipo de plan preventivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas. El plan de contingencia propone una serie de procedimientos alternativos al funcionamiento normal de una organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa.

Esta clase de plan, por lo tanto intenta garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad, ya sean materiales o personales. Un plan de contingencia incluye cuatro etapas básicas: la evaluación, la planificación, las pruebas de viabilidad y la ejecución.

Los especialistas recomiendan planificar cuando no es necesario, es decir, antes de que sucedan los accidentes. Un plan de contingencia debe permitir incluir alternativas frente a nuevas incidencias que se puedan producir con el tiempo, es por esto que debe ser actualizado de forma periódica.

### **6.2 PLAN DE CONTINGENCIA EN EL ÁREA DE TI.**

Consiste en la identificación de aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la organización, con el propósito de estructurar y ejecutar aquellos procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible y a unos costos razonables.

El plan de contingencia debe cubrir todos los aspectos que se van a adoptar tras una interrupción, lo que implica suministrar el servicio alternativo y para lograrlo no solo se deben revisar las operaciones cotidianas, sino que también debe incluirse el análisis de los principales distribuidores, clientes, negocios y socios, así como la infraestructura en riesgo. Esto incluye cubrir los siguientes tópicos: hardware, software, documentación, talento humano y soporte logístico; debe ser lo más detallado posible y fácil de comprender.

## 6.3 ETAPAS PARA ELABORAR UN PLAN DE CONTINGENCIA EN EL ÁREA DE TI.

### 6.3.1 Análisis y valoración de Riesgos

En primer lugar se debe realizar un análisis del impacto que causaría en la organización una falla e incidente en la plataforma tecnológica o un desastre natural. Se identifican los procesos críticos y las consecuencias que se presentan en caso de no estar en funcionamiento. El primer componente del Plan de Contingencia debe ser una descripción del servicio y el riesgo para ese servicio. También es recomendable determinar el costo que representa para la organización experimentar estos incidentes.

La evaluación del nivel de riesgo de la información sirve para:

- Determinar la relación costo/beneficio y tener argumentos para decidir entre aceptar la pérdida de información o invertir en implementar sistemas de contingencia.
- Clasificar los componentes de la plataforma tecnológica en términos de riesgo (alto, medio, bajo) e identificar aquellos que representen mayor riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio.
- Determinar la información que pueda representar pérdidas considerables para la organización o que impida una adecuada toma de decisiones.

Este análisis de posibles riesgos permitirá identificar las fortalezas, oportunidades, debilidades y amenazas, y profundizar en las medidas que se deben tomar para gestionirlas, de manera que en caso de incidentes se pueda recuperar la operatividad en el menor tiempo posible.

### 6.3.2 Jerarquización de las aplicaciones:

Es indispensable definir con anticipación cuáles son las aplicaciones primordiales para la organización. Teniendo en cuenta que para cada departamento o área funcional de la organización, su operación es la más importante, la jerarquización debe estar avalada y respaldada por un comité de contingencia o por la alta dirección, procurando objetividad y minimizando el conflicto de intereses.

El plan debe incluir una lista de los sistemas, aplicaciones y prioridades, así como identificar aquellos elementos informáticos (hardware, software base,

software de aplicaciones, telecomunicaciones) que puedan ser críticos ante cualquier incidente o desastre, jerarquizándolos de acuerdo al orden de importancia dentro de la organización. Se deben incluir los problemas generados por ausencia de fuentes de energía, mala administración o uso de dispositivos de backup o cualquier otro daño de origen físico que pueda provocar la pérdida masiva de información.

#### 6.3.3 Establecimiento de requerimientos de recuperación:

Esta etapa busca determinar lo que se debe hacer para lograr una óptima solución, especificando las funciones con base en el estado actual de la organización. Es necesario realizar las siguientes actividades: profundizar la definición del problema, analizar áreas o componentes problema, comunicaciones y sus flujos, formulación de medidas de seguridad necesarias dependiendo del nivel de seguridad requerido, justificación del costo de implantar las medidas de seguridad, análisis y evaluación del plan de contingencia actual (si lo hay), determinar los recursos humanos, técnicos y económicos necesarios para desarrollar el plan, definir un tiempo prudente y viable para lograr que el sistema se libere y pueda entrar en operación.

#### 6.3.4 Ejecución:

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante eventualidades que se puedan presentar con posterioridad. En esta etapa se debe tener presente que el plan de contingencia no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la empresa.

Para garantizar el éxito del plan de contingencia es conveniente que en su elaboración participen la alta dirección de la organización, personal técnico y operativo de los procesos y los usuarios, ya que los recursos necesarios para la puesta en marcha del plan, demandan mucho esfuerzo técnico, económico y organizacional y se requiere observar el sistema, la plataforma tecnológica y la operación de la compañía desde diversos puntos de vista.

#### 6.3.5 Pruebas y simulaciones:

Es necesario definir y generar simulaciones que permitan poner a prueba el plan de contingencia, el personal y los recursos necesarios para su realización. El propósito es intentar valorar el impacto real de un problema dentro de los escenarios establecidos como posibles. En caso de que los resultados

obtenidos difieran de los esperados, se debe analizar si el resultado varió por un problema en el ambiente de pruebas del plan, en cuyo caso se podrá corregir el problema y repetir la prueba, o si el plan tiene vacíos o carencias en su definición. Es indispensable la capacitación y participación del equipo de contingencia para detectar y evidenciar posibles carencias del plan, así como una buena documentación para facilitar la ejecución de las pruebas.

#### 6.3.6 Documentación:

Aunque esta etapa demanda un esfuerzo significativo, ayudará a comprender otros aspectos del sistema y puede ser apoyo para la empresa en caso de ocurrir un incidente o desastre. Debe incluir los procedimientos detallados que expliquen el paso a paso de las tareas de instalación y recuperación necesarias, procurando que sean entendibles y fáciles de seguir.

La documentación del plan de contingencia se debe desarrollar a medida que se avanza en la definición del plan y desde el mismo momento que nace, pasando por todas sus etapas; en ningún caso se debe dejar de lado esta labor, esperando a realizarla cuando se concluyan las pruebas y su difusión, pues se correría el riesgo de que la documentación resulte inexacta, difusa y que cualquier aspecto importante se pase por alto.

#### 6.3.7 Difusión y mantenimiento

Con el plan de contingencia probado y documentado, surge la necesidad de su difusión y capacitación entre las personas encargadas de llevarlo a cabo. El mantenimiento del plan comienza con una revisión del plan existente y se examina en su totalidad realizando los cambios en la información que pudo haber ocasionado una variación en el sistema y realizando los cambios que sean necesarios. La generación del plan no muere aquí, por el contrario es el inicio de un ciclo de revisión, ajuste y divulgación constante que suministre a la organización la tranquilidad de estar preparada y lista ante cualquier incidente.<sup>1</sup>

---

<sup>1</sup> <http://www.cibersociedad.net/congres2006/gts/comunicacio.php?id=309>

## 6.4 PLANES DE RESPALDO

### 6.4.1 Respaldo interno:

Las soluciones de respaldo interno tienen como objeto resolver contingencias leves que no precisen el desplazamiento fuera de los locales donde están ubicados los elementos informáticos afectados.

Cuando se trata del respaldo interno, generalmente las soluciones buscan uno o varios de estos objetivos:

- Redundancia de elementos (en ocasiones, disponer de más de un elemento con el fin de sustituir al que deja de funcionar, también puede considerarse como redundancia).
- Evitar los puntos únicos de fallo.
- Alta Disponibilidad.

### 6.4.2 Respaldo externo:

Tiene como objeto resolver contingencias graves (desaparición del edificio, desaparición del CPD, la avería de una plataforma, etc.), que precisan el desplazamiento a ubicaciones diferentes a la habitual (los denominados centros de respaldo alternativo o CAR).

Estas soluciones se aplican cuando la gravedad de la contingencia es tal que las soluciones de respaldo interno no se pueden aplicar, bien porque no cubran la contingencias, bien porque las instalaciones han quedado inoperantes para su uso.

Para que las soluciones de respaldo externo se apliquen, hay que pasar por un proceso de toma de decisión a resultas del cual se decida pasar a lo que se denomina modo contingencia, o lo que es lo mismo, se decide activar el Plan de Contingencias informáticas (PCI).

## 6.5 TIPOS DE CONTINGENCIA DE ACUERDO A LOS DAÑOS SUFRIDOS

Menor.- Es la que tiene repercusiones sólo en la operación diaria y se puede recuperar en menos de 8 horas.

Grave.- Es la que causa daños a las instalaciones, pero pueden reiniciar las operaciones en menos de 24 horas.

Crítica.- Afecta la operación y a las instalaciones, este no es recuperable en corto tiempo y puede suceder por que no existen normas preventivas o bien porque

estas no son suficientes. También puede suceder por ocurrir algún tipo de desastre natural como un terremoto.

#### 6.6 TIPOS DE CONTINGENCIAS DE ACUERDO AL GRADO DE AFECTACIÓN

- En el mobiliario y equipo.
- En el equipo de cómputo en general (procesadores, unidades de disco, impresoras etc.).
- En comunicaciones (hubs, routers, nodos, líneas telefónicas).
- Información.
- Instalaciones.

#### 6.7 GRUPO DE TRABAJO Y DEFINICIÓN DE ROLES PARA LA PREPARACIÓN DEL PLAN DE CONTINGENCIA

Se debe establecer formalmente el Comité del Plan de Contingencia con la siguiente estructura:

- Presidente del Grupo de Trabajo del Plan de Contingencia.
- Coordinador General.
- Coordinador de Redes y Comunicaciones.
- Coordinador de Soporte Técnico.
- Coordinador de Sistemas.
- Personal Clave.

##### 6.7.1 Presidente del Grupo de Trabajo:

Es el responsable de aprobar la realización del Plan de Contingencia Informático, dirigir los comunicados de concientización y solicitud de apoyo a los jefes y/o gerentes de las diferentes áreas involucradas y aprobar su terminación. Una vez concluida la realización del Plan de Contingencia, el Presidente tendrá como función principal, verificar que se realicen reuniones periódicas, por lo menos cada seis meses, en donde se informe de los posibles cambios que se deban efectuar al plan original y de que se efectúen pruebas del correcto funcionamiento del Plan de Contingencia Informático, al menos dos veces al año o antes si se presentan circunstancias de cambio que así lo ameriten.

Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alternativo y autorizará las inversiones a realizar así como el fondo de efectivo a asignarse para los gastos necesarios iniciales. El presidente se mantendrá permanentemente informado respecto de la activación del Plan hasta la declaración de conclusión.

#### 6.7.2 Coordinador General:

Tendrá como función principal asegurar que se lleven a cabo todas las fases para la realización del Plan de Contingencia, registrará las reuniones que se realicen, a manera de anotaciones, aprobará los procesos críticos y tipo de evento que abarcará el Plan de Contingencia y aprobará junto con el Presidente del Comité la terminación de cada una de las fases y la conclusión del proyecto. Durante la realización del plan, una de sus actividades principales será la coordinación de la realización de las pruebas del Plan de Contingencia, la aprobación de las ubicaciones alternas que sea necesario definir, la aceptación de los gastos y/o adquisiciones o contratos de servicios que sean necesarios para la realización del plan. Al término de la realización de las pruebas, será el Coordinador General quién dé su visto bueno de la conclusión de éstas y de sus resultados, rindiendo un informe a todos los coordinadores involucrados y en general al personal involucrado, y en caso necesario, convocar a la realización de una segunda prueba, corrigiendo previamente las fallas que se hubieran presentado. Una vez que se encuentre aprobado el Plan de Contingencia, será el Coordinador General quien lleve a cabo formalmente la declaración de una contingencia grave y dé inicio formal de la aplicación del Plan de Contingencia, cuando así lo considere conveniente, propiciando que la contingencia desaparezca con el objeto de continuar normalmente con las actividades; será el responsable de dar por concluida la declaración de contingencia.

#### 6.7.3 Coordinador de Redes y Comunicaciones:

Es el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, Servicios de Internet, Intranet, correo electrónico y red de la empresa, mantener actualizados dichos procedimientos en el Plan de Contingencia, determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, líneas telefónicas, cuentas de acceso a Internet, enlaces dedicados, dispositivos de comunicación (ruteadores, switchs, antenas etc.). Asimismo, deberá mantener actualizado el inventario de equipo de Telecomunicaciones y redes, efectuar los respaldos correspondientes y llevar acabo las pruebas de operatividad necesarias, para asegurar la continuidad del servicio, en caso de que se llegara a presentar alguna contingencia, ya sea parcial, grave o crítica. El Coordinador de Comunicaciones es el responsable de mantener el directorio de contactos, proveedores y usuarios de los servicios antes descritos y mantenerlo permanentemente actualizado e incluirlo dentro del Plan de Contingencia Informático. Coordinará las actividades correspondientes a los servicios de comunicaciones al declararse una contingencia, hasta su restablecimiento total.

#### 6.7.4 Coordinador de Soporte Técnico:

Es el responsable de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, CD Writer, escáners, faxes, copiadoras, etc.; mantener los equipos en óptimas condiciones de funcionamiento; determinar la cantidad mínima necesaria de equipo y sus características para dar continuidad a las operaciones de la empresa; es responsable de elaborar o coordinar con los usuarios los respaldos de información. Deberá realizar los procedimientos correspondientes para la emisión de los respaldos de cada uno de los servidores o equipos en donde se procese lo enunciado en el párrafo anterior, efectuar y mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, refacciones y desarrollo de software, en su caso, e incluirlo dentro del Plan de Contingencia Informático. En caso de que se declare alguna contingencia que afecte a los equipos y al software, sea cual fuere su grado de afectación, es el responsable de restablecer el servicio a la brevedad, con el objeto de que no se agrave el daño o se llegara a tener consecuencias mayores. Para tal efecto debe participar en pruebas del Plan de Contingencia en conjunto con los demás participantes, con el objeto de estar permanentemente preparado para actuar en caso de contingencia.

#### 6.7.5 Coordinador de Sistemas:

Será el responsable de determinar los sistemas Críticos de la Empresa, que en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, falla del sistema de cómputo, pérdida de documentación, o alguna otra causa determinada, se llegara a afectar sensiblemente la continuidad de las operaciones en las áreas que utilicen dichos sistemas críticos. En caso de cambiar a otras instalaciones alternas, el Coordinador de Programación deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación. Deberá mantener actualizados los Manuales Técnicos y de Usuario, resguardándolos fuera de las instalaciones para su consulta y utilización al momento de requerirse.<sup>2</sup>

---

<sup>2</sup> <http://es.scribd.com/doc/43714047/Plan-de-contingencia-sistemas-informaticos>



## 7. CRONOGRAMA DE ACTIVIDADES

**GRÁFICO 3. Cronograma de actividades.**

Actividades	Enero		Febrero				Marzo				Abril				Mayo				Junio				Julio		
	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3
A1																									
A2																									
A3																									
A4																									
A5																									
A6																									
A7																									
A8																									
A9																									
A10																									

Fuente: elaboración propia

A1: Inducción en la empresa

A2: Inducción en la Subgerencia de TI

A3: Visita del tutor de práctica y asignación del proyecto de a elaborar en la empresa.

A4: Elaboración y entrega del informe de ubicación

A5: Desarrollo y elaboración del informe de Plan de práctica.

A6: Entrega del informe al tutor y ultimas correcciones al plan de práctica.

A7: Diseño del plan de contingencia.

A8: Efectuar los planes propuestos en el plan de contingencia.

A9: Desarrollo, elaboración y entrega de los avances del informe de practica evidenciados en la ejecución del plan de contingencia.

A10: Ultimas correcciones y entrega del informe final del proyecto de práctica.

## 8. PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

Durante el proceso de práctica se han venido realizando varias funciones, de las que se destaca el proceso del plan de contingencia; a continuación se evidenciarán los procesos que se están realizando en las diferentes funciones del área además del análisis y planificación del plan de contingencia del área de TI de Une telefónica de Pereira.

### 8.1 PLANIFICACIÓN Y DISEÑO DEL PLAN PREVENTIVO Y REACTIVO

En el diseño del plan preventivo y reactivo de Une Telefónica de Pereira, se ha venido renovando la información del documento “Plan de Contingencia Subgerencia TI”; un documento contenido por el área de TI de la empresa que ayuda a estar preparados con anticipación a cualquier suceso que pueda afectar los sistemas de información de la empresa.

En este documento se actualizaron los datos de los principales proveedores del área de TI, debido a que a la hora de necesitar soporte ya sea del hardware o software, es importante tener los datos donde puedan ser contactados; también se actualizó la documentación con respecto a los cambios que se han generado en los diferentes servidores, debido a que mientras se revisaba la información contenida en ellos se observó que faltaba información y ya actualizados fueron agregados en el repositorio Tortoise SVN (Aplicación que almacena documentación de la empresa haciendo un control de versiones) y en la página de documentación de infraestructura TI <https://web.une.com/rsi/documentacion/menu.php> se actualizó la lista de los switches que están disponibles para hacer contingencia de los cuales se tomó el modelo, el serial y el tipo de puertos que contenían.

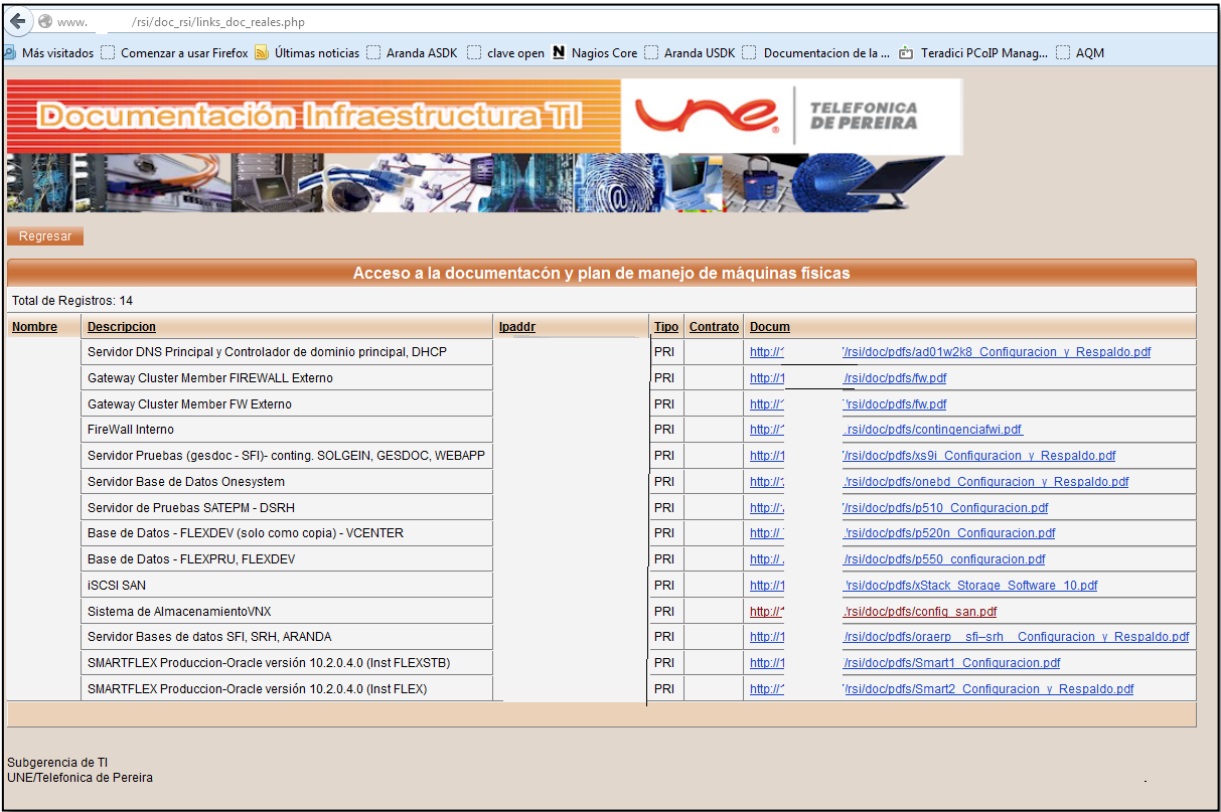
A continuación se muestran unas imágenes de lo mencionado anteriormente:

GRÁFICO 4. Página de documentación switches.



Fuente: www.etp.corp

GRÁFICO 5. Página de documentación servidores.




Fuente: página de documentación de la empresa

**GRÁFICO 6. Documentación almacenada en Tortoise SVN (aplicación para el control de versiones).**

svn://fsmr02.etp.corp.servidores/documentacion servidores

File	Extension	Revision	Author	Size	Date	Lock
esquemas		23	arios		08/04/2013 04:01:10 p.m.	
[F] Actualizar FLEXDEV_Oct_012.doc	.doc	14	arios	5,73 MB	17/10/2012 05:17:30 p.m.	
[F] ad01w2k8_Configuration_y_Respaldo.doc	.doc	1	arios	1,97 MB	26/07/2012 10:37:20 a.m.	
[F] backup and recover exchange2010.docx	.docx	28	arios	1,28 MB	17/04/2012 02:19:08 p.m.	
[F] Config FW Interno.docx	.docx	15	arios	2,09 MB	03/12/2012 12:27:32 p.m.	
[F] config_ad01w2k8.doc	.doc	1	arios	422 KB	26/07/2012 10:37:20 a.m.	
[F] config_antivirus.doc	.doc	1	arios	34,0 KB	26/07/2012 10:37:20 a.m.	
[F] config_fs.doc	.doc	1	arios	45,0 KB	26/07/2012 10:37:20 a.m.	
[F] config_boss.doc	.doc	1	arios	102 KB	26/07/2012 10:37:20 a.m.	
[F] config_onebd.doc	.doc	27	arios	124 KB	12/04/2013 02:59:48 p.m.	
[F] config_onegu.doc	.doc	1	arios	104 KB	26/07/2012 10:37:20 a.m.	
[F] config_onemed.doc	.doc	1	arios	43,0 KB	26/07/2012 10:37:20 a.m.	
[F] config_p510.doc	.doc	1	arios	62,5 KB	26/07/2012 10:37:20 a.m.	
[F] config_p520n.doc	.doc	30	arios	103 KB	20/05/2013 05:02:22 p.m.	
[F] config_p550.doc	.doc	1	arios	91,0 KB	26/07/2012 10:37:20 a.m.	
[F] config_san.doc	.doc	1	arios	219 KB	26/07/2012 10:37:20 a.m.	
[F] config_sf.doc	.doc	1	arios	102 KB	26/07/2012 10:37:20 a.m.	
[F] config_sf_srh.doc	.doc	10	arios	159 KB	24/09/2012 11:47:20 a.m.	
[F] config_sgetdbd.doc	.doc	1	arios	101 KB	26/07/2012 10:37:20 a.m.	
[F] config_smart1.doc	.doc	19	arios	140 KB	18/12/2012 10:10:15 a.m.	
[F] config_smart2.doc	.doc	4	arios	288 KB	13/09/2012 11:29:35 a.m.	
[F] config_ts.docx	.docx	25	arios	18,8 KB	08/04/2013 04:03:38 p.m.	
[F] config_vmail.doc	.doc	1	arios	62,5 KB	26/07/2012 10:37:20 a.m.	
[F] config_vvms.doc	.doc	1	arios	33,5 KB	26/07/2012 10:37:20 a.m.	
[F] config_zsrf.doc	.doc	1	arios	201 KB	26/07/2012 10:37:20 a.m.	
[F] contingencia de switches de distribucion y acceso.doc	.doc	31	arios	35,0 KB	23/05/2013 04:36:08 p.m.	
[F] contingencia Switches de Core (Cisco 4507).doc	.doc	32	arios	446 KB	23/05/2013 04:36:42 p.m.	
[F] Diagrama de conexión Equipo de VideoConferencia ETP.pdf	.pdf	20	arios	143 KB	16/01/2013 03:31:42 p.m.	
[F] Documentación Instalación plataforma EMC y Brocade.pdf	.pdf	24	arios	1,50 MB	08/04/2013 04:01:30 p.m.	
[F] Esquema_Racko_Alamos_Corea.JPG	.JPG	5	arios	44,5 KB	13/09/2012 12:22:14 p.m.	
[F] Esquema_Racko_Centro.JPG	.JPG	6	arios	30,8 KB	13/09/2012 12:22:28 p.m.	
[F] Esquema_Racko_Centro1.JPG	.JPG	7	arios	49,0 KB	13/09/2012 12:22:41 p.m.	
[F] Esquema_Racko_Centro2.JPG	.JPG	8	arios	59,9 KB	13/09/2012 12:22:52 p.m.	
[F] Esquema_SAN_bds.JPG	.JPG	9	arios	91,4 KB	13/09/2012 12:23:10 p.m.	
[F] Plan de Contingencia TI.doc	.doc	29	arios	1,80 MB	15/05/2013 05:40:48 p.m.	


  
servidores

Fuente: foto tomada a aplicación empresarial

### 8.1.1 Formatos plan de contingencia

A continuación se muestran las plantillas que se llenaron como parte de la documentación de la empresa al plan de contingencia mostrando el número de prueba, el equipo al cual se le va a comprobar la contingencia, el tipo de prueba que se va a ejecutar, las fechas de realización y los responsables de su ejecución.

Este formato se llenó con respecto a las necesidades del área de TI de la empresa, poniendo en primer lugar los servidores primordiales que permiten el continuo desenvolvimiento laboral al interior de la empresa con el fin de comprobar su estado al momento de que ocurra algún acontecimiento inesperado y se necesite como respaldo.

## GRÁFICO 7. Formato Plan de recuperación de Backups.

<b>PLAN DE CONTINGENCIA SUBG. TI</b> <b>PLAN DE RECUPERACIÓN DE BACKUPS AÑO 2013 Primer Semestre</b>							
Amenaza	Nro. Prueba	Elemento	Equipo	Prueba	Fecha Propuesta	Fecha Realizada	Responsable
Falla en cualquier elemento físico	1	Servidor	Fm5w3k20	Recuperar el backup de un usuario (backup de pc)	Junio 7		
	2	Servidor	Smt1	Recuperar un <u>export</u> semanal de la BD Smt1	Junio 11		
	2	Servidor	finanzas bk	Recuperar un <u>export</u> semanal del FINANZAS	Junio 17		
	4	Servidor (virtual)	ESis	Recuperar formas de HUMANAS de \apps\apps del backup más reciente	Junio 25		
	5	Servidor	Finanzas	Recuperar la <u>bd</u> HUMANAS completa a partir del último <u>export</u>	Junio 29		

Fuente: elaboración propia

Ya habiendo diligenciado los primeros 5 campos del Plan de recuperación de backups se procederá a su ejecución donde todo lo evidenciado debe quedar debidamente plasmado en el siguiente formato, documentando la fecha de ejecución, número de prueba, tipo de prueba, elemento de prueba, descripción de la prueba, responsable y asistentes de la prueba, hora inicial y final, y por último y lo más relevante la descripción de eventos y/o inconvenientes obtenidos durante la prueba para mostrar en qué estado se encuentra la contingencia al interior de la empresa y poder dar soluciones y correcciones pertinentes.

## GRÁFICO 8. Formato pruebas plan de contingencia.

		<b>PRUEBAS PLAN DE CONTINGENCIA</b> <b>Subgerencia de T.I</b>		Página de Nro Prueba:	
Fecha :					
<b>Datos</b>					
Tipo de Prueba			Elemento de la Prueba		
Descripción de prueba:					
Responsable de la Prueba					
Asistentes					
Hora Inicial:			Hora Final:		
Descripción de eventos y/o inconvenientes tenidos durante la prueba					
Solicitante		Responsable		Solicitante	

Fuente: elaborado por la empresa.

### 8.2 AUDITORÍA ESTADO DE EJECUCIÓN DE BACKUPS

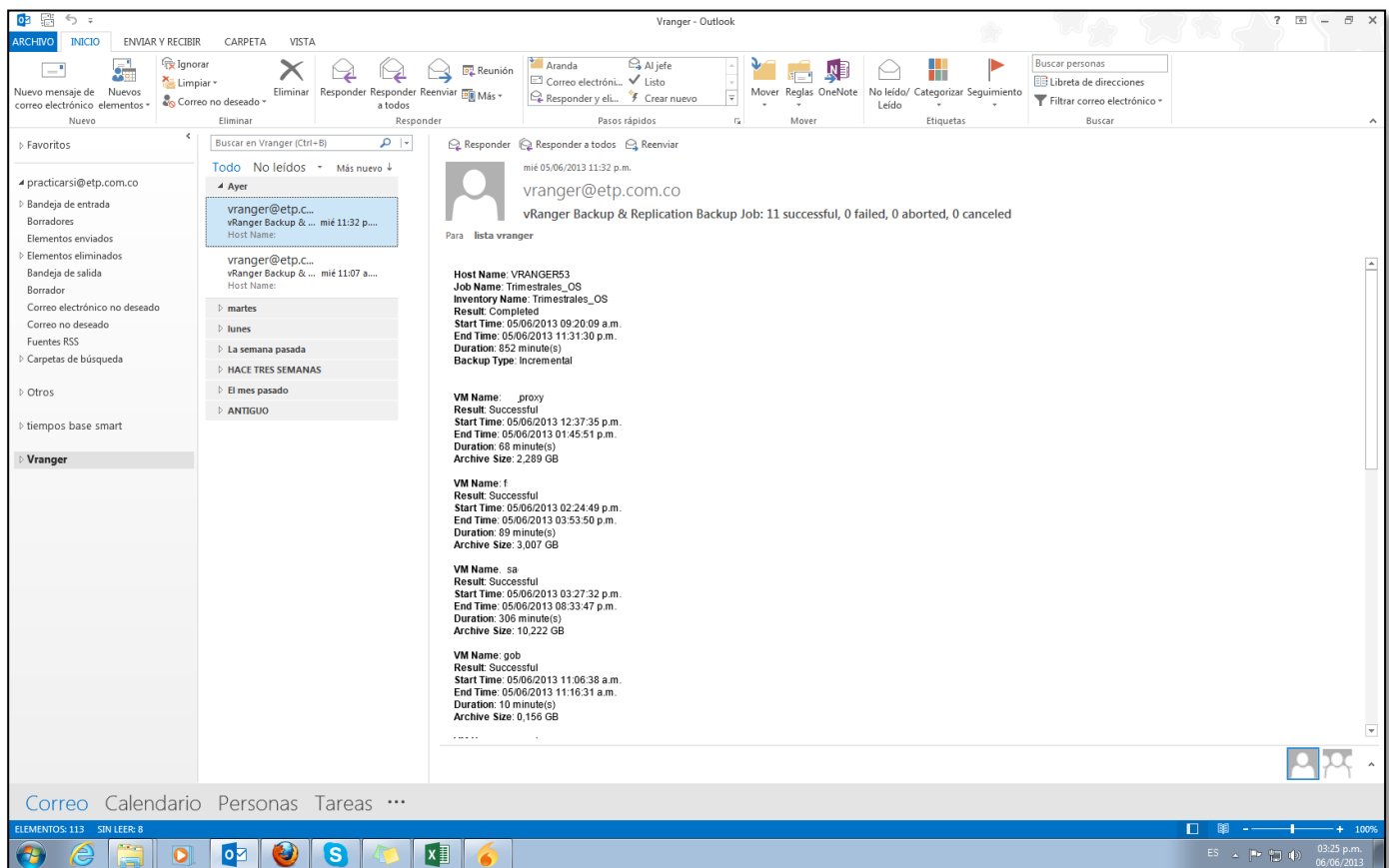
Diariamente al correo empresarial practiacarsi@etp.com.co llega el listado de los backups que se ejecutan en los diferentes servidores de la infraestructura virtual de la empresa, mostrando su estado de ejecución successful, failed, canceled y aborted, para tener un control del éxito o del fracaso de los backups, teniendo siempre información actualizada para estar preparados ante cualquier acontecimiento y que la información pueda ser recuperada, fomentando de esta forma un tipo de contingencia al interior de la empresa.

#### 8.2.1 Backup vRanger:

Uno de los correos que se recibe tiene por nombre Vranger (solución de protección de datos número 1 de VMware, que además realiza copias de seguridad y recuperación a servidores físicos con Windows y archivos con los

requisitos mínimos de velocidad y almacenamiento). Con vRanger, se obtiene una protección completa para entornos físicos y virtuales que se pueden gestionar desde una única interfaz intuitiva (VMware vSphere Client); al recibir el correo Vranger divididos en diarios, semanales, mensuales bimensuales y trimestrales, la practicante documentó la información allí obtenida para llevar un control de la misma, registrándola en la bitácora de backup Vranger ubicadas en el directorio Y:\Log\BitacorasBKS\bkVranger documentando por fecha su estado de ejecución (successful, failed, aborted, canceled) y en caso de no ser exitosa la ejecución del backup, informar las posibles causas de la falla y así realizar las correcciones pertinentes y retomar el backup con la información actualizada y en buen estado, adquiriendo una contingencia para cada servidor de la infraestructura virtual de la empresa.

## GRÁFICO 9. Correo vRanger.



Fuente: foto tomada al correo empresarial.

**GRÁFICO 10. Bitácora backups vRanger.**

Backups Marzo 2013		V	S	D	L	MA	MI	J	V	S	D	L	MA	MI	J	V	S	D	L	MA	MI	J	V	S	D	L	MA	MI	J
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Diario	onm_be	ok			ok	ok	ok	ok	ok			ok	ok	ok	ok	ok			ok	ok	ok	ok	ok			ok	ok	ok	ok
	onm_le	ok			ok	ok	ok	ok	ok			ok	ok	ok	ok	ok			ok	ok	ok	ok	ok			ok	ok	ok	ok
Semanal	ascu1							ok							ok						ok								ok
	ascu2							ok							ok						ok								ok
	epitra25							ok							ok						ok								ok
	fwlgmt							ok							ok						ok								ok
	solg							ok							ok						ok								ok
	mon							Aborted							ok						ok								ok
	wep							ok							ok						ok								ok
Quincenal	a50dt2k8	ok														ok													
	arcuis	ok														ok													
	dbv	ok														ok													
	nombres	ok														ok													
	hos21	ok														ok													
	icc10	ok														ok													
	spc	ok														ok													
	vcs801	ok														ok													
	Johnny	ok														ok													
	wepext	ok														ok													

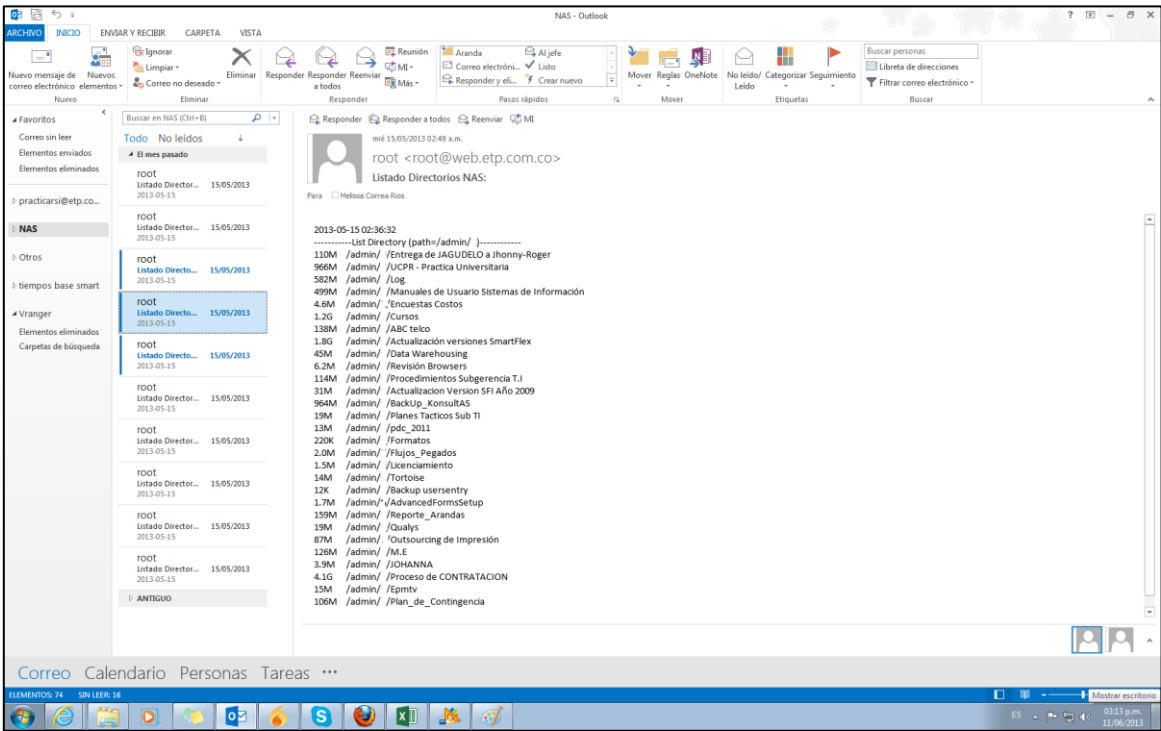
Fuente: elaboración propia

### 8.2.2 Backup Directorios NAS y freeNAS:

Al correo también llega el listado de los directorios NAS (servidor de acceso a la red), los servidores NAS permiten a los usuarios acceder a la red y almacenar en los discos de estos servidores la información que usen a nivel empresarial. Al igual que con el correo Vranger, la información que allí llegó fue registrada dentro del proceso de práctica, en una bitácora cada 15 días, en donde por fecha se registraron los directorios que cada disco tiene y el tamaño con el que cuenta cada uno para tener un control de la cantidad de archivos que se manejan en cada uno y el crecimiento de estos, corroborando que su información no sea alterada por otros, perjudicando la información de la empresa visualizando el tamaño de los archivos que allí se encuentran.



GRÁFICO 11. Correo directorios NAS.



Fuente: foto tomado a correo empresarial

GRÁFICO 12. Bitácora repositorio NAS.

	A	J	K	L	M	N	O	P	Q
1									
2	DIRECTORIO	ENERO	Enero	FEBRERO	MARZO	MARZO	ABRIL	ABRIL	MAYO
3		15	30	15	15	30	15	30	15
4	/usr	2.9G	2.9G	2.9G	2.9G	2.9G	2.9G	2.9G	2.9G
5	/net	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K
6	/p4	20K	20K	20K	20K	20K	20K	20K	20K
7	/pi3	20K	20K	20K	20K	20K	20K	20K	20K
8	/boot	6.2M	6.2M	6.2M	6.2M	6.2M	6.2M	6.2M	6.2M
9	/sys	0	0	0	0	0	0	0	0
10	/proc	0	0	0	0	0	0	0	0
11	/root	249M	249M	249M	249M	249M	249M	249M	249M
12	/home	19M	19M	19M	19M	19M	19M	19M	19M
13	/lost+found	16K	16K	16K	16K	16K	16K	16K	16K
14	/etc	108M	108M	108M	108M	108M	108M	108M	108M
15	/tmp	151M	151M	151M	151M	151M	151M	151M	151M
16	/dev	172K	172K	172K	172K	172K	172K	172K	172K
17	/pi4	501G	501G	501G	501G	501G	501G	501G	501G
18	/p1	266G	266G	266G	266G	750G	883G	883G	883G
19	/var	819M	825M	831M	842M	931M	903M	910M	916M
20	/selinux	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K
21	/srv	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K	8.0K
22	/pi1	501G	501G	501G	501G	501G	501G	501G	501G
23	/lib	76M	76M	76M	76M	76M	76M	76M	76M
24	/pi2	20K	20K	20K	20K	20K	20K	20K	20K
25	/cc	1.3T	1.3T	1.3T	1.3T	1.4T	40G	3.1G	3.1G

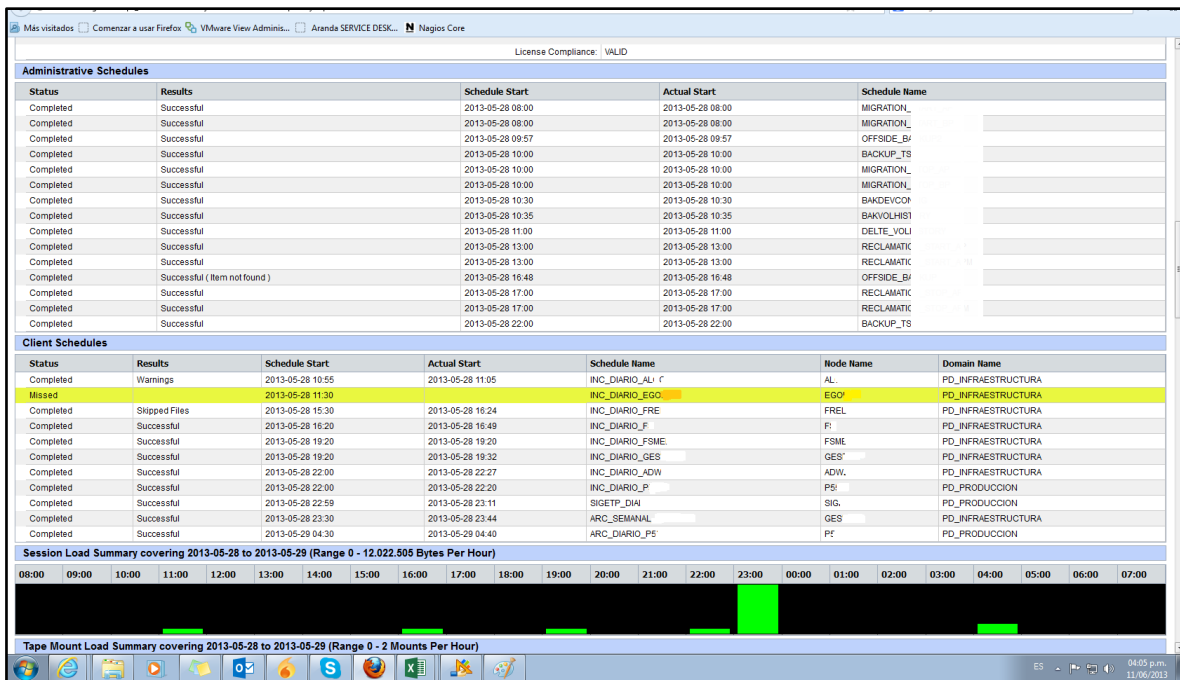
Fuente: elaboración propia

### 8.2.3 Backup TSM:

Tivoli Storage Manager (TSM) o más recientemente llamado IBM Tivoli Storage Manager (ITSM) es un software centralizado y basado en políticas que permite la administración de los recursos de almacenamiento ofreciendo protección de datos automatizada y centralizada para reducir los riesgos asociados con la pérdida de datos.

Al interior de la empresa se cuenta con este software, el cual almacena y protege los datos de cada uno de sus empleados, para este software también se ejecutaba un correo, el cual llegaba diariamente a las 7:00 am a la practicante mostrando el estado de la ejecución del backup, tal y como se muestra a continuación (Grafico 11 y 12) donde diariamente en el semestre de practica se procedió a llenar la bitácora según si fue exitoso su estado de ejecución o de lo contrario, llenarla con lo sucedido (equipo apagado, falla en la contraseña, activación del firewall, error de servicios, falta de espacio en el storage pool, etc. ) y se informaba para realizar las correcciones pertinentes:

### GRÁFICO 13. Informe backup TSM.



Fuente: foto tomada a página web empresarial

## GRÁFICO 14. Bitácora backups TSM.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1					<b>BACKUPS RESPALDADOS EN SERVIDOR TSM</b>											
2		inc_diario_al	inc_diario_eg		inc_diario_fre	inc_diario	inc_diario_fsr	inc_diario_ges	inc_diario_adw	inc_diario_pt	getp_diario	arc_diario_p	arc_semanal_ge	arc_semanal_p	getp_sei	arc_mensual
3	miércoles	1	apagado	apagado	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok		
4	jueves	2	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok		
5	viernes	3	apagado	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok		
6	sábado	4			ok	ok	ok	ok	ok	ok	ok	ok	ok	ok		
7	domingo	5			ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
8	lunes	6	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
9	martes	7	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
10	miércoles	8	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
11	jueves	9	apagado	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
12	viernes	10	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
13	sábado	11			ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
14	domingo	12			ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
15	lunes	13	apagado	apagado	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
16	martes	14	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
17	miércoles	15	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
18	jueves	16	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
19	viernes	17	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
20	sábado	18			ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
21	domingo	19			ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
22	lunes	20	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
23	martes	21	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
24	miércoles	22	ok	ok	ok	error servidor	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
25	jueves	23	ok	apagado	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
26	viernes	24	ok	error clave	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
27	sábado	25			ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
28	domingo	26			ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
29	lunes	27	ok	apagado	ok	ok	ok	ok	servicio suspendido	ok	ok	ok	ok	ok	ok	ok
30	martes	28	ok	servicio suspendido	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
31	miércoles	29	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall	se activo firewall
32	jueves	30	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok	ok
33	viernes	31	ok	ok	ok	ok	ok	ok	ok	error_password	ok	ok	ok	ok	ok	ok

Fuente: elaboración propia

### 8.3 CONTROL DE SOFTWARE CON ARANDA SOFTWARE METRIX®

ASM es una herramienta diseñada para administrar efectivamente las licencias, y por consiguiente, la legalidad del software instalado en las estaciones de trabajo de la empresa. Con el uso dado a la plataforma “ASM” o Aranda SOFTWARE METRIX®, se ha reducido en más del 80% el software no permitido instalado en la empresa donde periódicamente se desinstalaron aquellos que no fueran admitidos al interior de la empresa y que no tuvieran licenciamiento.

## GRÁFICO 15. Control de licenciamiento por aplicación.

The screenshot displays the Aranda Software Metrix application window. The interface includes a sidebar with navigation options like 'Licenciamiento', 'Sistema Operativo', 'Aplicaciones', 'Contrato', 'Factura', and 'Alarmas'. The main area shows a table of software licenses with columns for 'Estación', 'Nombre del equipo', 'Estado', 'Versión agente', 'Descripción', 'Usuario', 'Grupo de trabajo', 'Dominio', 'Servidor', and 'Número de procesadores'. The table lists various software products such as AUTOCAD, MICROSOFT OFFICE, and other business applications, along with their respective users and server information.

Estación	Nombre del equipo	Estado	Versión agente	Descripción	Usuario	Grupo de trabajo	Dominio	Servidor	Número de procesadores
8214	ROLANDO CAMARGO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CARLOS M. OSORIO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MARGARITA MARIA PALACIO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CAROLINA FREDERITA URIBE	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ALEX HENAO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MARLUZ RODAS	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ADRIANA MARTINEZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	LIZ ANDREA GALLEGO G.H	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ANA MARIA CASTRO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MANUEL ALEJO CARDONA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ANA BEATRIZ MEJIA - FACTUR	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MARCELA ACEVEDO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MARTALIA ANDREA ARANGO M	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ANDREA MANDEZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ANGELA MARULANDA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	BRENA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ARACELLY DUSSAN	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ANGIE RENGIFO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	AVILLADA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	ANGELA VELASQUEZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CALL 18	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CAROLINA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CAROLINA PAQUE	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CLARA MENICA CEBALLOS	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	JUAN FELIPE GRAJALES	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MARIA EUGENIA GONZALEZ L	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CLAUDIA VALENCIA FACTURA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CLAUDIA A. LOPEZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	EHUMIR SALAZAR ROJAS ZON	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CARLOS ALBERTO RAMIREZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	FRANCY LINARES	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	DIANA MARCELA MENA ACEVE	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	HAYDIVER VALENCIA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	LADY JOHANNA VELASQUEZ L	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CLAUDIA MARIA CALVO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	SANDRA LOPEZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	JULIANA MARTINEZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	LINA HERNANDEZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	CESAR AUGUSTO HERNANDEZ	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	JOHANNA LOPEZ AGUDELO	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MARIA CRISTINA ZAPATA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MARIA EUGENIA GONZALEZ L	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1
8214	MARIA ELENA MARULANDA	ETP	ETP	ETP	ETP	ETP	ETP	ETP	1

Fuente: foto tomada a aplicación empresarial Aranda Metrix

Aranda Metrix tiene como función primordial el manejo de inventarios de software que tiene la empresa, con esta excelente ayuda el encargado de la administración del software en la empresa puede tener el total control del software y administrar también el número de licencias con las que cuenta la empresa de un determinado aplicativo.

ASM se encarga de monitorear el uso del software en las estaciones de una empresa y organizar la información obtenida. El agente local Aranda instala el módulo Metrix en cada estación, el cual revisa continuamente todas las ejecuciones de software que se llevan a cabo, detectando para cada programa el tiempo que tarda en ejecutarse. Utilizando este agente y toda la información recolectada, ASM puede determinar cómo se está utilizando el software instalado en cada PC (<http://www.arandasoft.com>).

Una vez monitoreado cada pc automáticamente por el software Aranda, semanalmente el practicante evaluó cada una de las aplicaciones instaladas, valorando si estas eran permitidas o no según su licenciamiento y de forma manual se categorizaron distribuyéndolas de la siguiente manera: Actualizaciones de Windows, Adicionales office, Adobe, Antivirus, Bases de datos, Cisco,

Desinstalados, Desinstalar, Drivers, Empresarial, Incluido en equipos, Java, Mensajería, Navegadores, Software bancos, Software celulares y cámaras, Software libre, Software ofimático, para tener un control del software instalado; siendo primordial el software que se debe desinstalar para que no existieran problemas de licenciamiento al interior de la empresa, debido a los derechos de autor en donde la empresa se podría ver afectada con multas por la instalación de software no licenciado.

**GRÁFICO 16. Clasificación del software en Aranda Software Metrix.**

Software	GRUPO	Incluida	Licenciado	Estacion
Actualizaciones Windows (2592)	Software Libre	NO	NO	4
Adicionales Office (104)	Software Libre	NO	NO	336
Adobe (84)	Software Libre	NO	NO	192
Antivirus (14)	Software Libre	NO	NO	13
Bases de datos (24)	Software Libre	NO	NO	425
Cisco (11)	Drivers	NO	NO	1
Desinstalados (961)	Software Libre	NO	NO	117
Desinstalar (196)	Software ofimático	SI	SI	9
Desinstalar1 (0)	Navegadores	NO	NO	116
Drivers (469)	Drivers	NO	NO	116
Empresarial (146)	Drivers	NO	NO	88
Incluido en equipos (319)	Actualizaciones Windows	NO	NO	80
Java (72)	Actualizaciones Windows	NO	NO	88
Mensajería (46)	Actualizaciones Windows	NO	NO	4
Navegadores (94)	Actualizaciones Windows	NO	NO	116
Software bancos (3)	Actualizaciones Windows	NO	NO	85
Software celulares y cámaras (83)	Actualizaciones Windows	NO	NO	71
Software Libre (361)	Actualizaciones Windows	NO	NO	66
Software ofimático (42)	Actualizaciones Windows	NO	NO	89
Software por Revisar (86)	Actualizaciones Windows	NO	NO	111
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB20794)	Actualizaciones Windows	NO	NO	59
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB21151)	Actualizaciones Windows	NO	NO	105
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB21215)	Actualizaciones Windows	NO	NO	115
ACTUALIZACIÓN PARA WINDOWS XP (KB2141007)	Actualizaciones Windows	NO	NO	3
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB21603)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS INTERNET EXPLORER 8	Actualizaciones Windows	NO	NO	4
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB22295)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB22599)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN PARA WINDOWS XP (KB2264107)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB22799)	Actualizaciones Windows	NO	NO	60
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB22861)	Actualizaciones Windows	NO	NO	111
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB22960)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB22961)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN PARA WINDOWS XP (KB2345886)	Actualizaciones Windows	NO	NO	111
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB23472)	Actualizaciones Windows	NO	NO	109
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS INTERNET EXPLORER 8	Actualizaciones Windows	NO	NO	2
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB23609)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA EL REPRODUCTOR DE VÍDEO DE WINDOWS XP	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB23871)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB23938)	Actualizaciones Windows	NO	NO	111
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24126)	Actualizaciones Windows	NO	NO	109
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS INTERNET EXPLORER 8	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24196)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24230)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24366)	Actualizaciones Windows	NO	NO	60
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24405)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24431)	Actualizaciones Windows	NO	NO	110
ACTUALIZACIÓN PARA WINDOWS XP (KB2467659)	Actualizaciones Windows	NO	NO	10
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24766)	Actualizaciones Windows	NO	NO	73
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24789)	Actualizaciones Windows	NO	NO	111
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24789)	Actualizaciones Windows	NO	NO	111
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24796)	Actualizaciones Windows	NO	NO	65
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24799)	Actualizaciones Windows	NO	NO	111
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS INTERNET EXPLORER 8	Actualizaciones Windows	NO	NO	2
ACTUALIZACIÓN DE SEGURIDAD PARA WINDOWS XP (KB24831)	Actualizaciones Windows	NO	NO	111

Fuente: foto tomada a aplicación empresarial Aranda Metrix

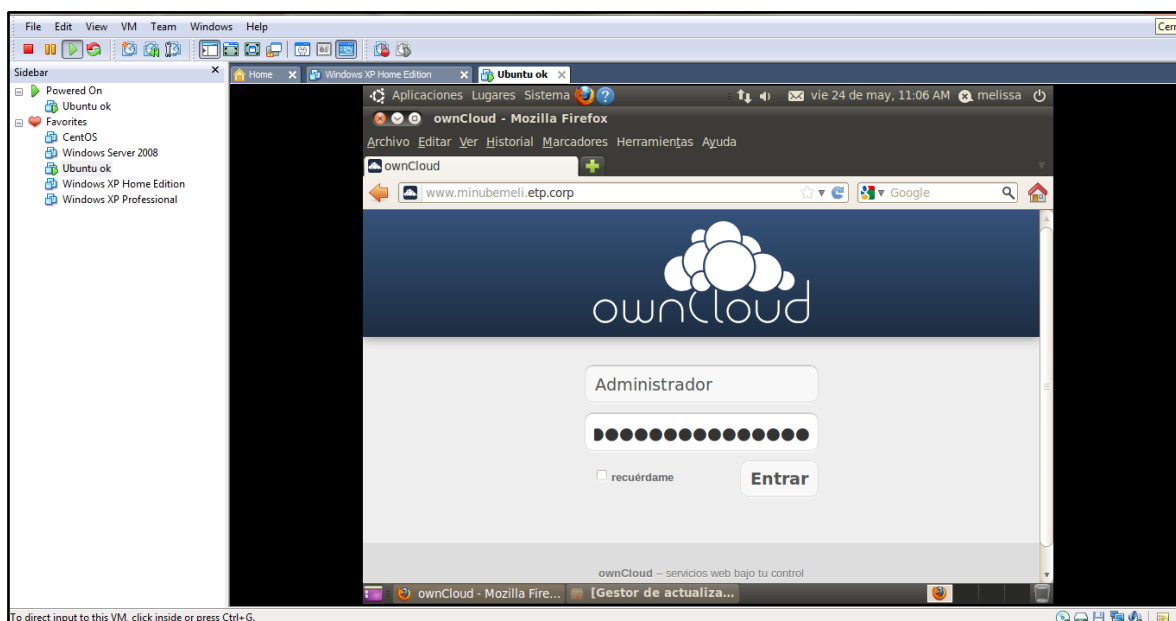
## 8.4 OWNCLOUD

Al inicio de la práctica se acordó como unas de las funciones, la implementación de la aplicación web OwnCloud, un software libre de almacenamiento independiente a la ubicación de los datos basado en la nube, como su nombre indica “OwnCloud”(nube propia) donde además del almacenamiento de datos,

también permite la sincronización de archivos entre diferentes dispositivos, teniendo la posibilidad de compartirlos poniendo a disposición servicios de reproductor de música, visor de imágenes, editor de texto plano, gestor de ficheros y marcadores a través de una interfaz Web.

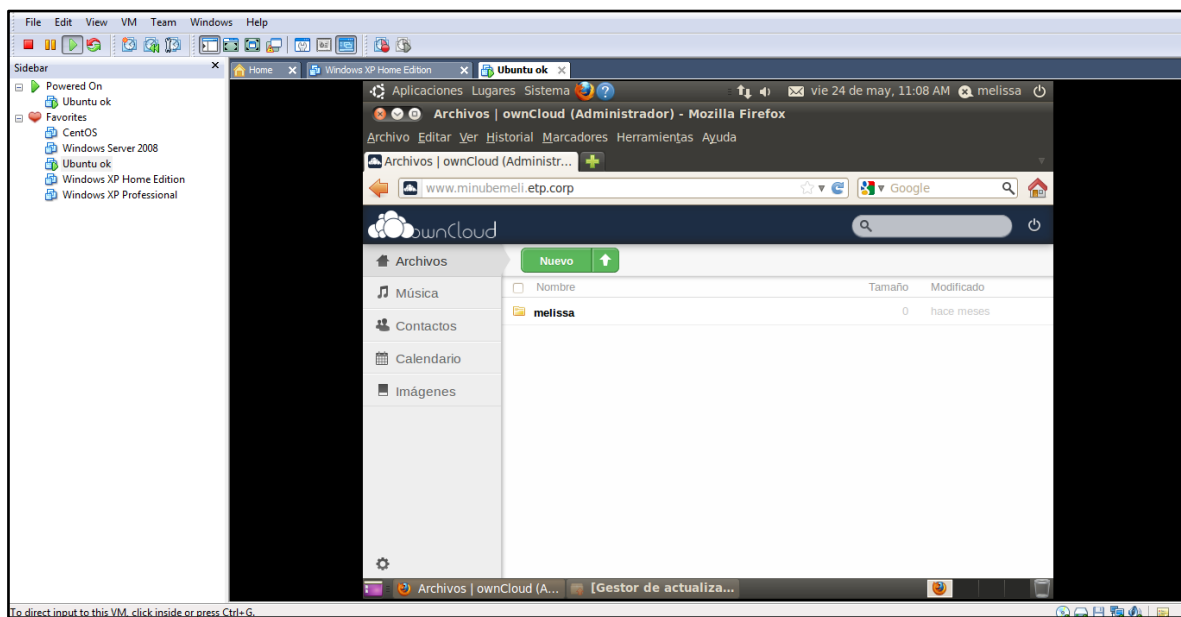
A través de una máquina virtual creada en la herramienta VMware Workstation se instaló el sistema operativo Ubuntu y desde allí se procedió a montar la página web por medio de comandos en Linux; una vez terminada esta parte se mostró el proyecto para continuarlo e implementarlo al interior de la empresa, pero por decisión de integrantes de TI y debido a que existen actualmente otras formas de almacenamiento se declinó el seguimiento de esta función pero que termino por ser de gran aprendizaje, ya que se tenía pocos conocimientos con respecto a comandos en Linux.

### GRÁFICO 17. OwnCloud logueo administrador.



Fuente: foto tomada a implementación propia

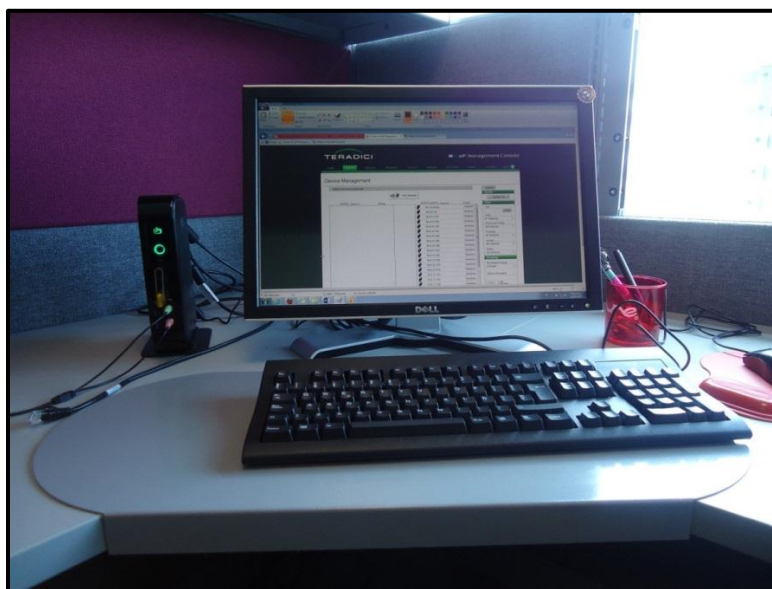
**GRÁFICO 18. OwnCloud Administración de la página.**



Fuente: foto tomada a implementación propia

## 8.5 VIRTUALIZACION DE ESCRITORIOS

**GRÁFICO 19. Equipo trabajando con la tecnología PCoIP.**



Fuente: foto tomada a puesto de trabajo en UNE



Al interior de la empresa se está empezando con la implementación de virtualización de escritorios utilizando thin clients con el fin de contar con los siguientes beneficios:

- **Ahorro:** Cero costo en mantenimiento de los equipos terminales.
- **Automatización:** Reducción de los tiempos y las tareas de aprovisionamiento.
- **Simplicidad:** Menor cantidad de recursos a administrar.
- **Costos:** Incremento de la vida útil de la red LAN, cero riesgo de pérdida de información ante fallos de energía.
- **Flexibilidad:** Independencia del PC.
- **Eficiencia:** Anchos de banda estandarizados.
- **Ecología:** Reducción del consumo energético.
- **Disponibilidad:** Permite reducir a cero las paradas programadas para mantenimiento de las máquinas.
- **Operación:** Administración centralizada de todas las máquinas.
- **Portabilidad:** Portabilidad de la máquinas virtuales entre servidores físicos.

#### 8.5.1 Thin Client

Una thin client (cliente liviano o cliente delgado) es una computadora cliente o un software de cliente en una arquitectura de red cliente-servidor que depende primariamente del servidor central para las tareas de procesamiento, y se enfoca principalmente en transportar la entrada y la salida entre el usuario y el servidor remoto.

**GRÁFICO 20. Dell Wyse P20 Zero Client.**



Fuente: foto tomada a equipo de trabajo



Una Telefónica de Pereira adquirió los equipos Dell Wyse P20 como computadoras cliente para la implementación de esta nueva tecnología donde durante el periodo de práctica se instalaron las siguientes thin client en cada sede de atención al cliente, emergiendo la empresa en una nueva y grandiosa tecnología.

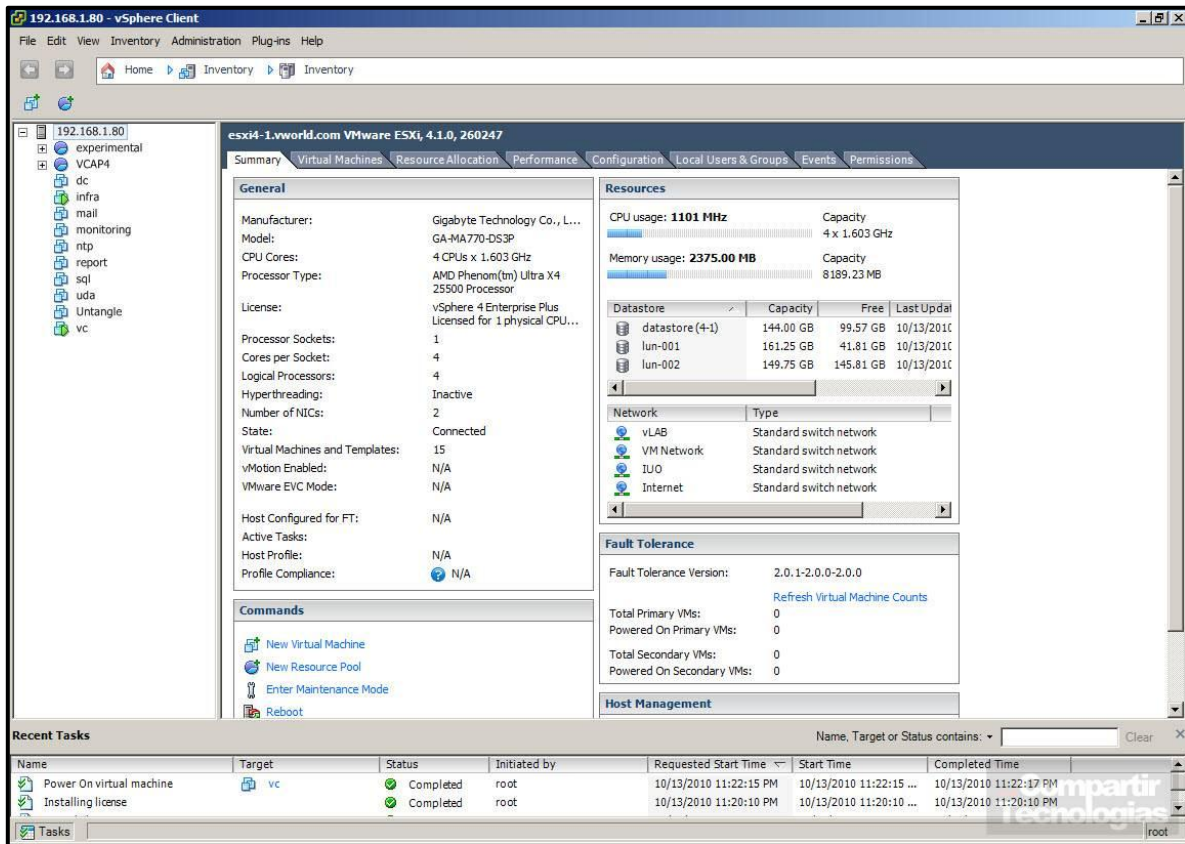
**GRÁFICO 21. Inventario de Thin Client instaladas por sede.**

SEDE	N° THIN CLIENT
Cuba	1
Dosquebradas	2
Telecliente victoria	23
Gerencia	1
subgerencia	1
Santa Rosa	3
call center	2
helpdesk	5
TI	3
ventas esquina	1
la Virginia	1
TOTAL	43

Fuente: elaboración propia

## 8.5.2 VMware vSphere Client

### GRÁFICO 22. Entorno de administración de virtualización VMware vSphere Client.



Fuente: [www.malaysiavm.com/blog/windows-7-on-vsphere](http://www.malaysiavm.com/blog/windows-7-on-vsphere)

Para la creación de los escritorios virtuales se está utilizando la herramienta VMware vSphere Client (plataforma de virtualización líder del sector para la creación de infraestructuras en la nube).

Se crearon 4 máquinas virtuales principales a las cuales se les instaló Windows 7 y las respectivas aplicaciones según la necesidad del área de trabajo; estas se mencionan a continuación:

GoldenGral: Máquina principal del centro de atención al cliente.

GoldenTI: Máquina principal del área de tecnologías de la información.

GoldenHdesk: Máquina principal del área de HelpDesk.

GoldenAdm: Máquina principal Gerencia y subgerencia.

A estas máquinas durante la práctica se les realizaron varias actualizaciones de acuerdo a peticiones de servicio debido a nuevas necesidades en el uso de algunas herramientas en un área de trabajo.

Para poder replicar y aplicar las actualizaciones a todos los equipos thin client, con el VMware vSphere client se le tomó a las máquinas principales un Snapshot o foto instantánea del estado del sistema en un momento determinado (copia real del estado de un sistema o de una capacidad que ofrecen los sistemas de copia de seguridad), los cuales fueron usados para replicar esta imagen a los usuarios y también se utilizaron como medio de contingencia para cuando los escritorios virtuales presentaron problemas con alguna nueva actualización.

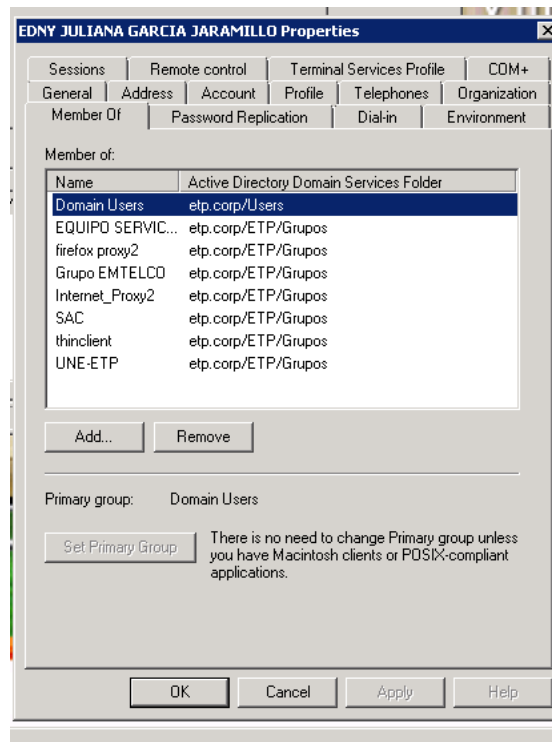
#### 8.5.3 Agregar un nuevo usuario al entorno virtual.

Durante el proceso de práctica una de las funciones que se asignaron para la virtualización de escritorios, fue el crear e incluir a usuarios dentro del entorno virtual y agregarle los ajustes necesarios, para aquellos que se les hiciera cambio de equipo y entregarle una thin client. Esta función se realizó de la siguiente manera.

##### A) INGRESO AL DIRECTORIO ACTIVO

Se ingresaba al servidor del directorio activo por acceso remoto y allí se buscaba el usuario deseado y en la pestaña **Member Of**, se agregaba a los grupos sac o subgerencia a la cual pertenecía, thin client y Firefox y finalmente en la pestaña Profile se agregaba la ruta de la unidad z: \\sf\smart.

### GRÁFICO 23. Adición a grupo Thin Client.



Fuente: foto tomada a AD de la empresa

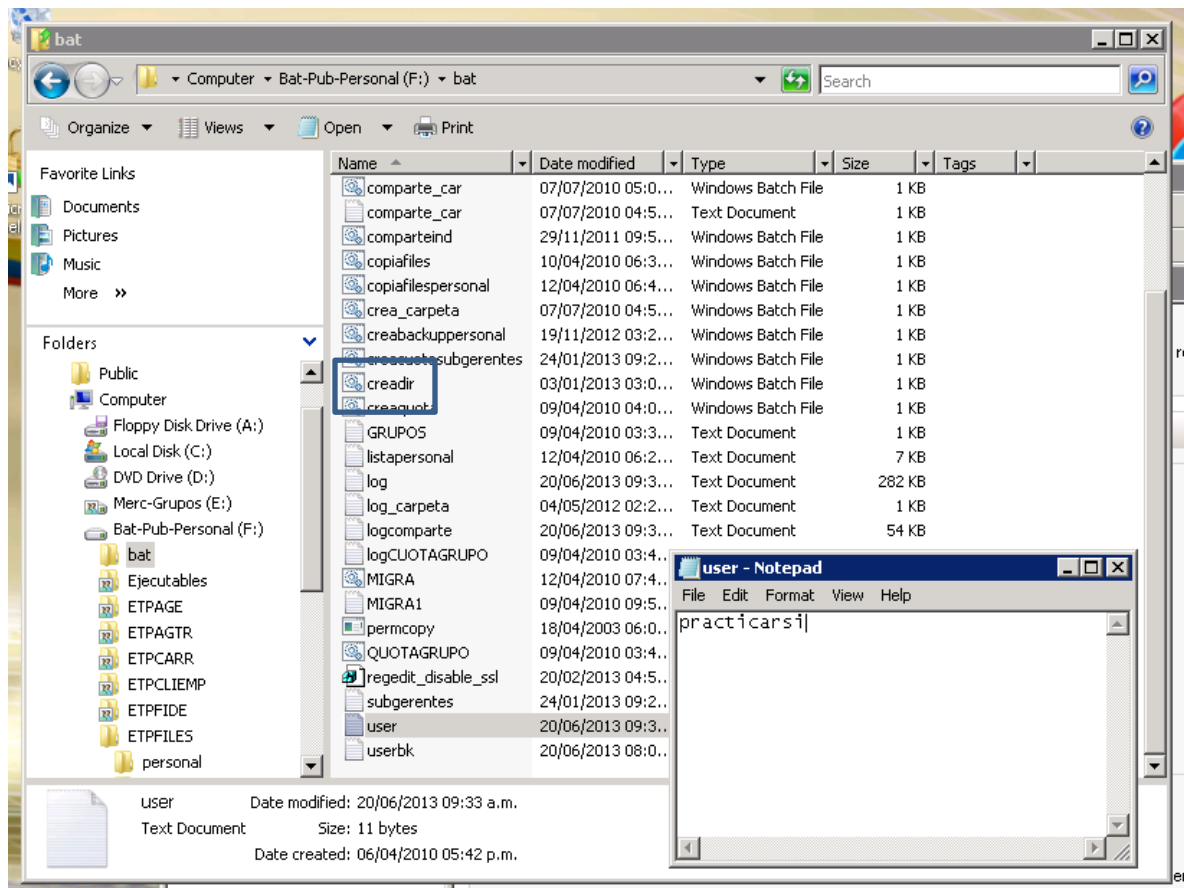
### B) CREACION DE UNIDAD PERSONAL CUOTA O BACKUP.

Luego se procedía con la creación de una unidad de red personal llamada backup donde ya creado se le pedía a los usuarios que almacenaron toda la información que utilizaban en la empresa para tener sus archivos siempre a salvo.

En este servidor se ingresaba a la ruta F:\ETPFILES\personal donde se encuentra creada la carpeta del backup con el nombre de usuario y se debía cerciorar que se encontrara compartida, y si no estaba incluida esta carpeta, se procedía con la creación de la misma de la siguiente manera:

Se dirigía a la ruta F:/ bat y se editaba el archivo user.txt ingresando los usuarios a los que se les iba a crear la carpeta personal y finalmente para que se crearla, se ejecutaba el archivo creardir.bat de esta forma se creaba la carpeta, la compartía y le asigna la cuota (cantidad de megas de disco asignado). Grafico 24.

## GRÁFICO 24. Carpetas personales o backup.



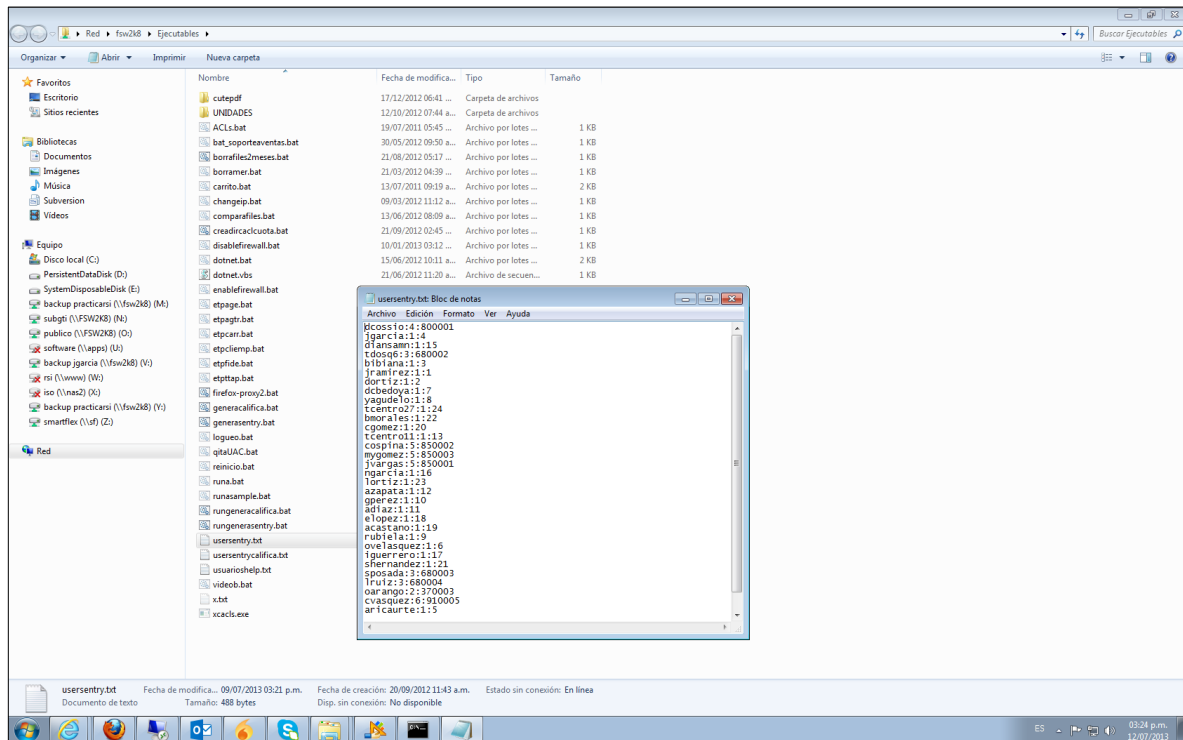
Fuente: foto tomada a equipo de la empresa

### C) CONFIGURACION SENTRY

Para el área de atención al cliente se debía configurar un software llamado Sentry que es el llamado a turno de atención al cliente.

Para configurarlo y permitir que cada usuario fuera registrado en la taquilla debida; se ingresaba a la ruta \\jlw7k8\ejecutables y allí se editaba el archivo llamado usersentry.txt en el siguiente orden para la ejecución de un script XML; nombre del usuario: id de la sede: número de la taquilla; así:

## GRÁFICO 25. Registro a Consola Sentry.

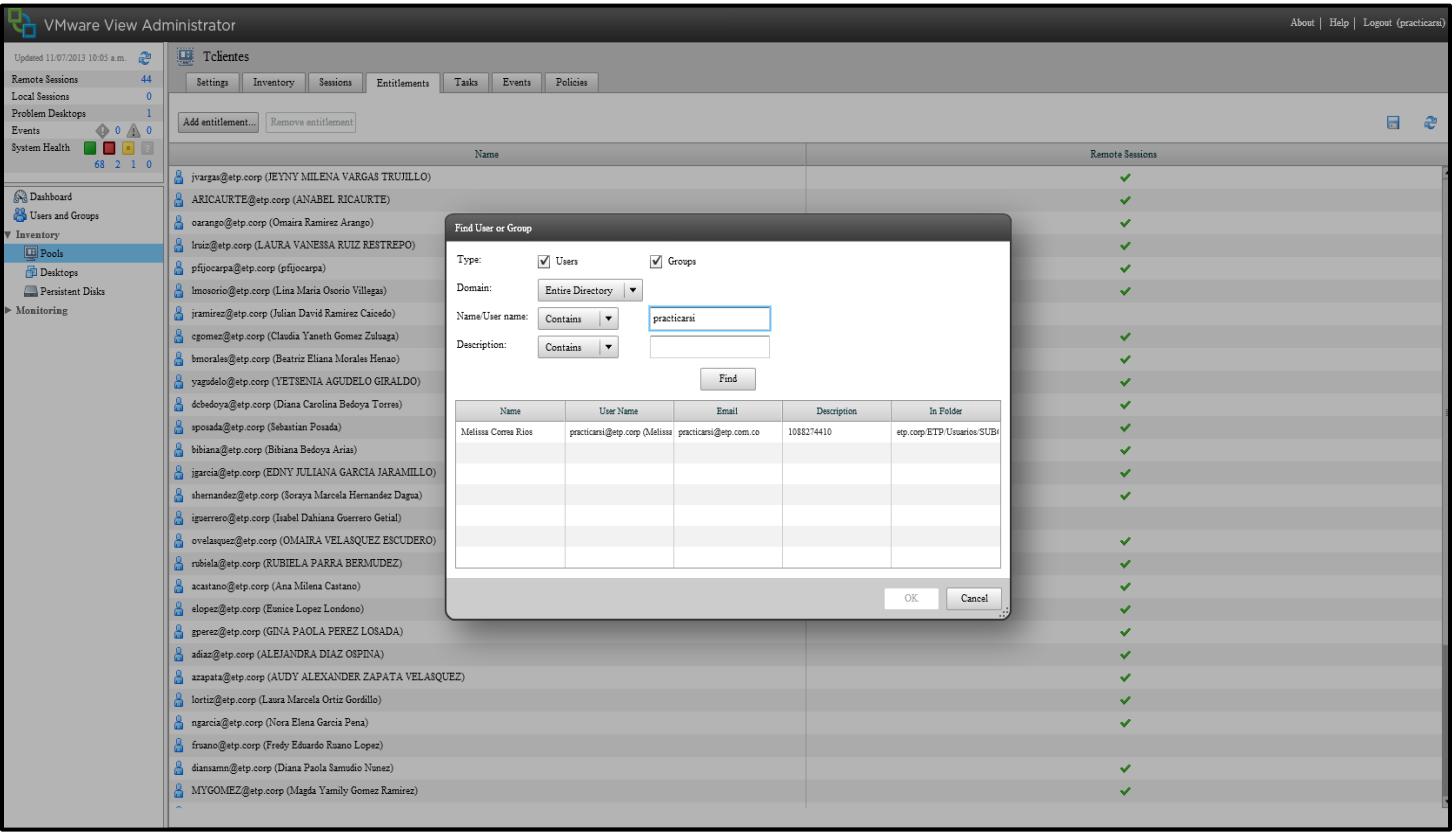


Fuente: Tomada en equipo de la empresa

### D) ENTITLEMENT

Para que un usuario quedara incluido en este entorno virtual se ingresaba a la consola de administración VMware View Administrator y desde allí se agregaba al pool correspondiente al área donde pertenecía el usuario y en una función de la consola de administración llamada entitlement se agregaba el usuario queriendo decir “Derecho a” y eso permitía que los usuarios ya fueran asignados al mundo de los escritorios virtuales.

GRÁFICO 26. Agregar Entitlement.



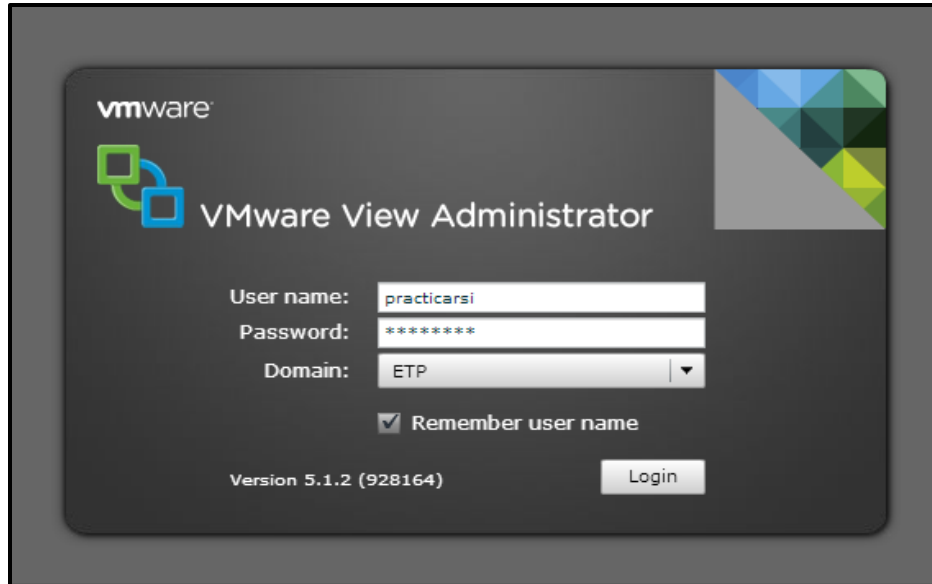
Fuente: <https://vcs.etp.corp>

8.5.4 Herramientas de administración de la virtualización de escritorios.

Para administrar los escritorios virtuales, se hizo uso de dos herramientas que permitían desde un solo lugar dar mantenimiento a las máquinas y virtualización para su perfecto funcionamiento. A continuación se da un breve repaso de sus funciones:

A. View Administrator.

**GRÁFICO 27. Ventana de logeo a VMware View Administrator.**



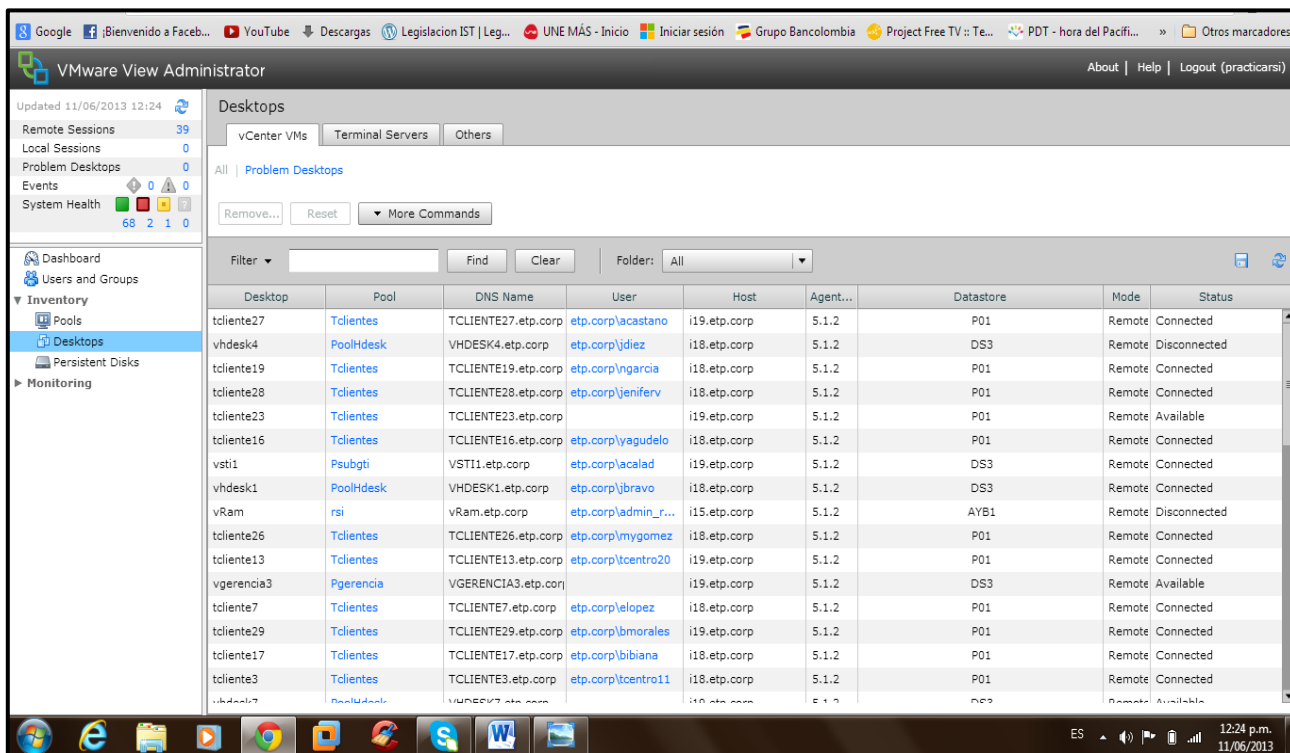
Fuente: <https://vcs.etp.corp>

VMware View Administrator se describe cómo configurar y administrar VMware View™, incluyendo cómo configurar View Connection Server, crear administradores, provisión y despliegue de Vistas de escritorio, configurar la autenticación de usuario, configurar políticas y administrar aplicaciones VMware ThinApp™ en la Vista de administrador. Esta información también se describe cómo mantener y solucionar problemas de componentes de VMware View. (VMware, inc., 2013)

Para la administración de estas máquinas se utilizó el entorno VMware view administrator, el cual proporciona todas las herramientas adecuadas para dar soluciones a todas las necesidades requeridas de esta tecnología.



## GRÁFICO 28. Entorno de administración VMware View.



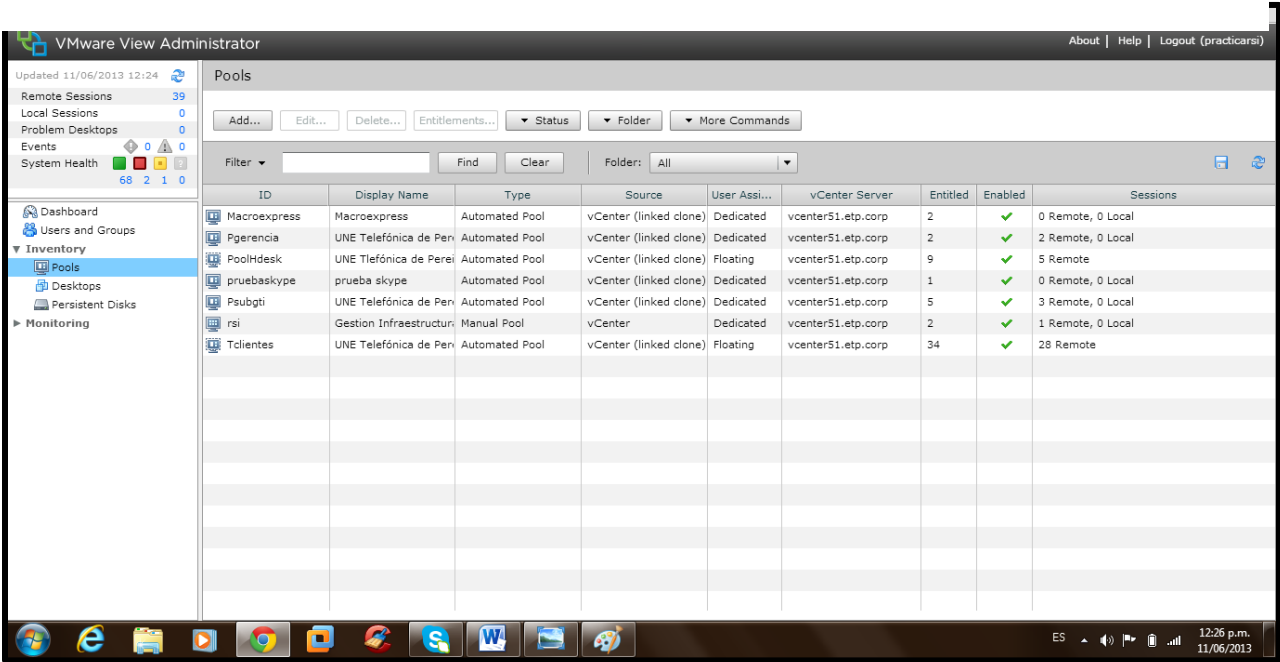
Fuente: <https://vcs.etp.corp>

Las funciones que cumple el entorno administrativo de virtualización de escritorios son:

### - Crear un pool:

Un pool de máquinas quiere decir un grupo de máquinas con las mismas características, dicho esto, en la empresa para la virtualización de escritorios se cuenta con 7 pools (Macroexpress, Pgerencia, PsubgtI, PruebaSkype, PoolHdesk, Tcliente y rsi; Grafico 29); de los cuales el pool con nombre prubaskype hecho con el fin de probar el funcionamiento de video y sonido en skype en esta tecnología, fue creado en el proceso de práctica donde se hicieron varias pruebas para configurar su correcto funcionamiento.

GRÁFICO 29. Pools.



The screenshot shows the VMware View Administrator web interface. On the left is a navigation pane with 'Inventory' expanded and 'Pools' selected. The main area displays a table of pools. Above the table are buttons for 'Add...', 'Edit...', 'Delete...', 'Entitlements...', 'Status', 'Folder', and 'More Commands'. A filter bar is also present. The table has columns for ID, Display Name, Type, Source, User Assignment, vCenter Server, Entitled, Enabled, and Sessions.

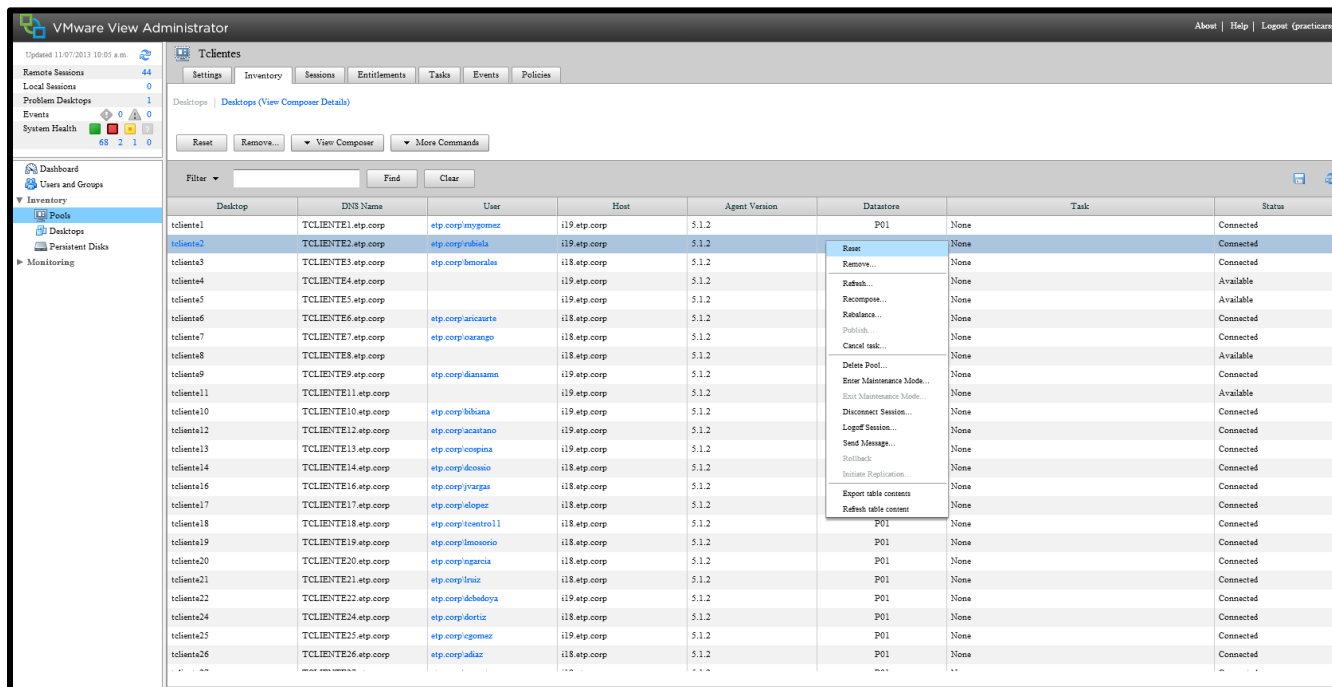
ID	Display Name	Type	Source	User Assi...	vCenter Server	Entitled	Enabled	Sessions
Macroexpress	Macroexpress	Automated Pool	vCenter (linked clone)	Dedicated	vcenter51.etp.corp	2	✓	0 Remote, 0 Local
Pgerencia	UNE Telefónica de Per	Automated Pool	vCenter (linked clone)	Dedicated	vcenter51.etp.corp	2	✓	2 Remote, 0 Local
PoolHdesk	UNE Telefónica de Perei	Automated Pool	vCenter (linked clone)	Floating	vcenter51.etp.corp	9	✓	5 Remote
pruebaskype	prueba skype	Automated Pool	vCenter (linked clone)	Dedicated	vcenter51.etp.corp	1	✓	0 Remote, 0 Local
Psubgti	UNE Telefónica de Per	Automated Pool	vCenter (linked clone)	Dedicated	vcenter51.etp.corp	5	✓	3 Remote, 0 Local
rsi	Gestion Infraestructur	Manual Pool	vCenter	Dedicated	vcenter51.etp.corp	2	✓	1 Remote, 0 Local
Tclientes	UNE Telefónica de Per	Automated Pool	vCenter (linked clone)	Floating	vcenter51.etp.corp	34	✓	28 Remote

Fuente: <https://vcs.etp.corp>

**- Reset:**

Se ejecutaba la funcion reset en el entono web de administración, para reinicializar una maquina cuando esta no respondía adecuadamente.

## GRÁFICO 30. Función Reset.



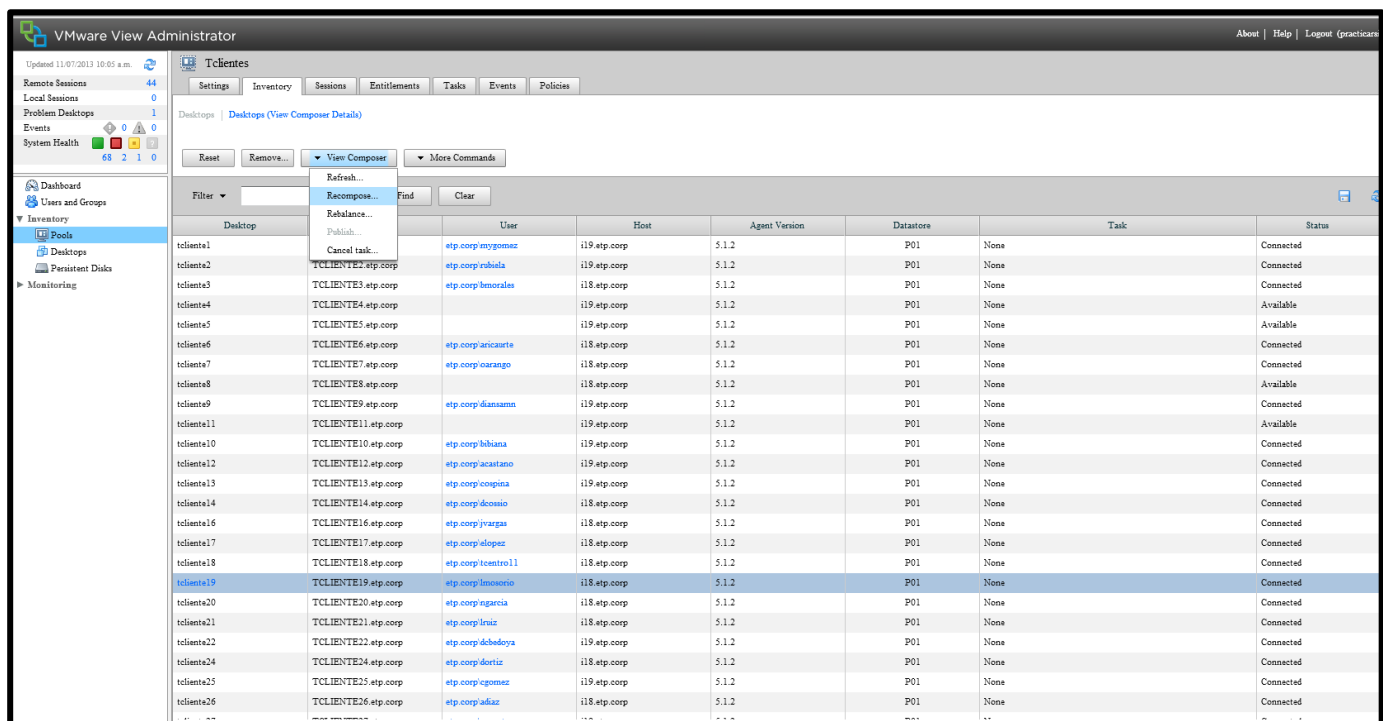
Fuente: <https://vcs.etp.corp>

### - Recompose:

En el periodo de práctica se ejecutó varias veces esta función, la cual permitía replicar a todos los escritorios virtuales todos los cambios hechos en las maquinas principales “Golden”. Por medio del recompose estas adquirirían las características o software instalado con solo hacerlo en la Golden por medio del VMware vSphere client, se le hacía un snapshot y finalmente se ejecutaba el comando recompose, se elegía el nuevo snapshot y ésta en tan solo 15 minutos actualizaba los cambios en todas los escritorios virtuales existentes.

Un ejemplo de este ejercicio se realizó con frecuencia durante la antepenúltima semana de práctica, ya que a los asesores de servicio al cliente se les instalo un nuevo software donde el cliente debe calificar el nivel de atención de servicio al cliente (de 1 a 5) y por esta razón se necesitó realizar un recompose y actualizarle este software en cada uno de sus escritorios.

## GRÁFICO 31. Función recompouse.



Fuente: <https://vcs.etp.corp>

### - Assign User:

Dentro de la administración de escritorios existen dos tipos de Pool, Pool dedicado y Pool flotante; el flotante hace que automáticamente cada que un usuario apague la máquina y la vuelva a encender le entregue un escritorio virtual diferente y a cambio del dedicado permite que una maquina siempre se relacione con un único usuario permitiendo así desde un principio asignárselo por medio de la función assign user.(Grafico 32) . Esta función se ejecutó 2 veces en el periodo de práctica; cuando se instalaron los equipos en el área de TI y en la Gerencia ya que para mejor administración y control de estas dos áreas se, decidió asignarle una única maquina a los usuarios.

Ejemplo:

En el área de TI existen 5 máquinas que fueron distribuidas de la siguiente forma:

Vsti1 → usuario arios (Albeiro Ríos)

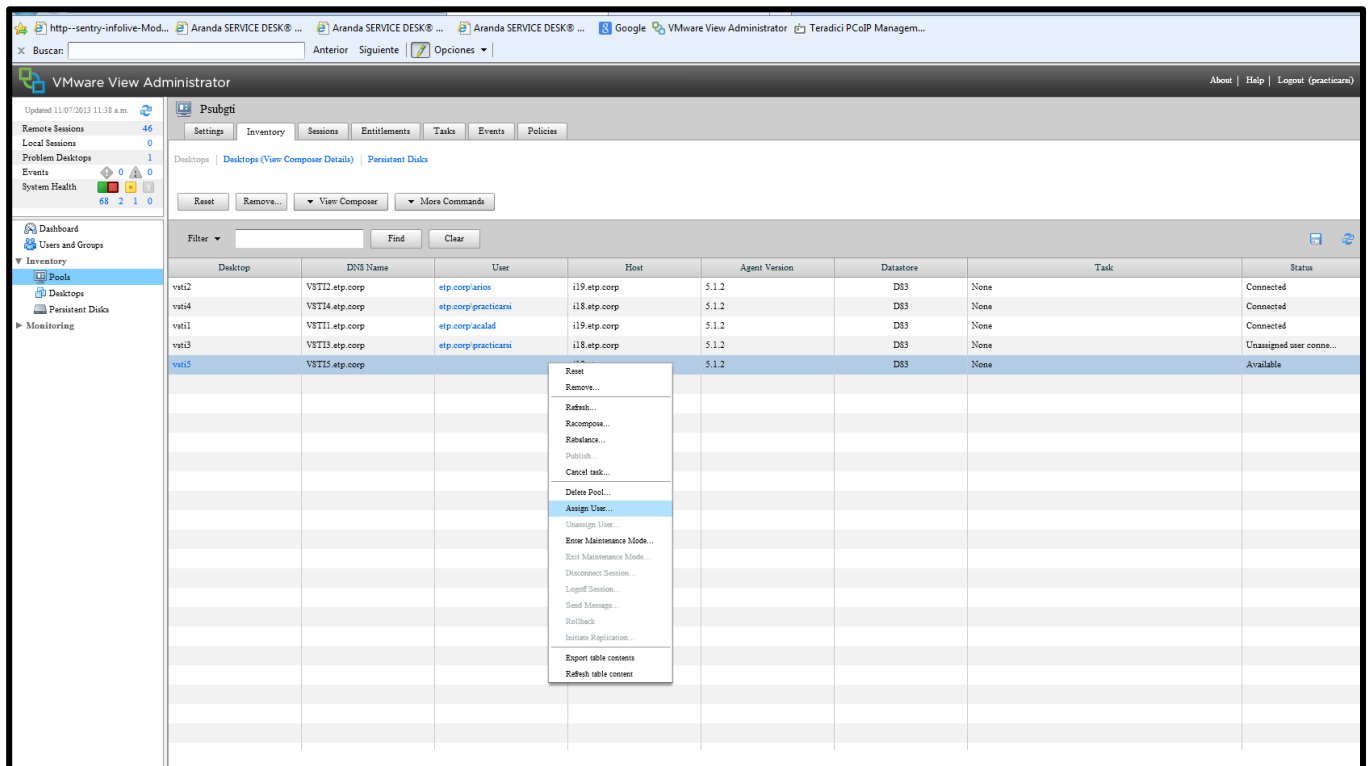
Vsti2 → usuario acalad (Alfredo Calad)

Vsti3 → Pruebas.

Vsti4 → usuario paracticarsi (Melissa Correa)

Vsti5 → aún está disponible para entregar al próximo usuario que se le dé una thin client.

### Grafico 32. Asignar usuario a una máquina específica.

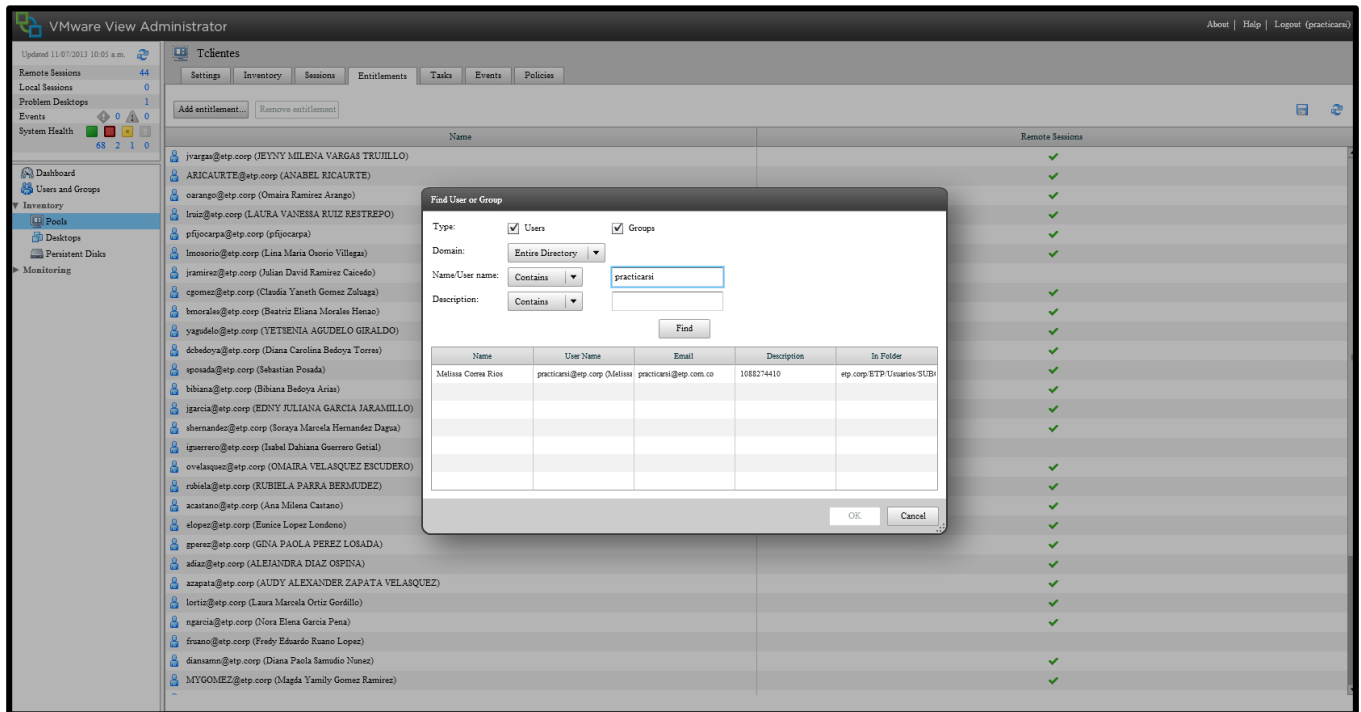


Fuente: <https://vcs.etp.corp>

#### - Entitlement:

Como ya se mencionó anteriormente, el entitlement cumple la función de darle permisos a un usuario de hacer parte de un entorno virtual, donde sin este derecho el usuario no tendría la forma de loguearse con sus usuarios en un equipo de virtualización o thin client.

## GRÁFICO 33. Entitlement.

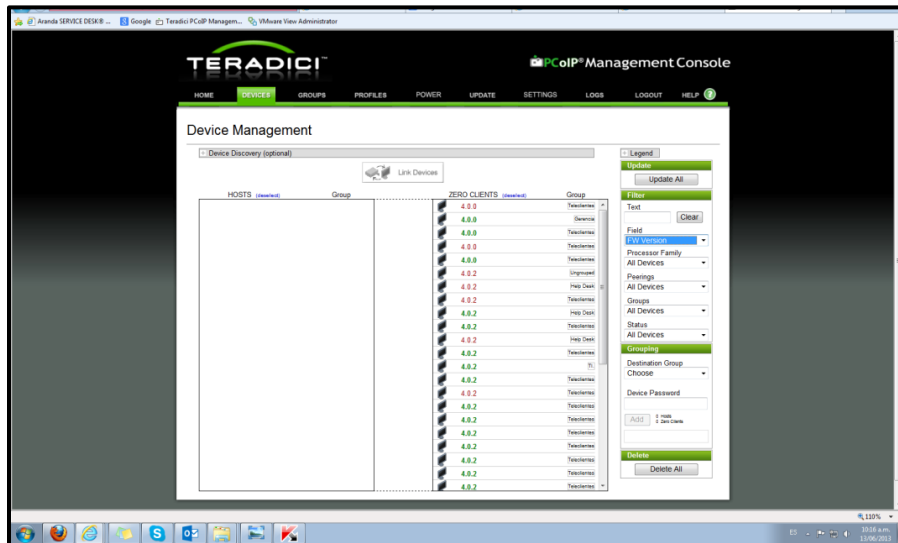


Fuente: <https://vcs.etp.corp>

### B. PCoIP Management Console

PCoIP Management Console es otro entorno de administración web que se utilizó en periodo de práctica para replicar cambios en los escritorios virtuales.

### GRÁFICO 34. Consola web para administración de PCoIP.



Fuente: <https://teradici.com>

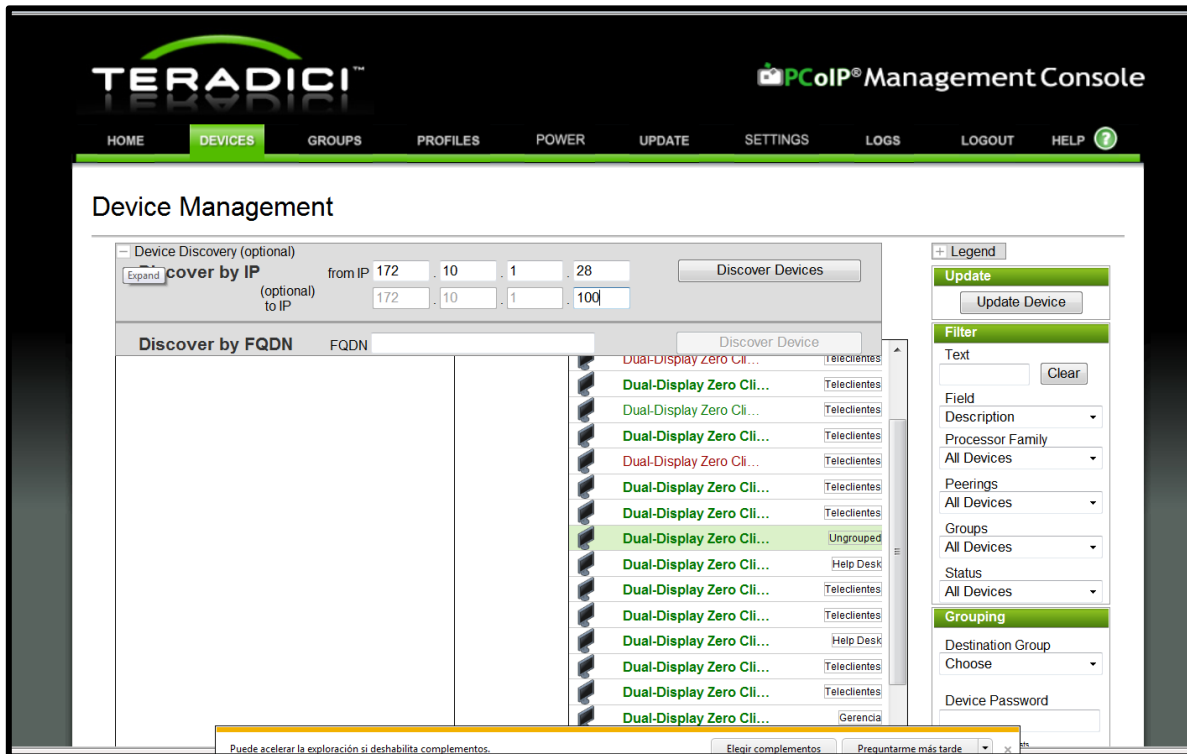
La Consola de administración de PCoIP es una herramienta de gestión basada en web que permite a los administradores implementar y administrar una implementación empresarial de muchos dispositivos PCoIP desde una consola central, una mayor racionalización de la gestión a un mínimo de infraestructura PCoIP (Teradici Corporation, 2013).

Por medio de esta consola semanalmente se administró los PCoIP de la siguiente manera:

- Configurando que automáticamente se descubran cuando estén en la red:

En el proceso de práctica se realizaron instalación de thin client en las áreas de servicio al cliente, en gerencia y en call center, donde cada que se instalaba una thin client se ponía en ejecución el descubrimiento y actualización de los dispositivos instalados tal y como se muestra en el Grafico 35, escribiendo el rango de direcciones ip pertenecientes al área para que esta consola web los rastreará en la red.

GRÁFICO 35. Escaneo de Dispositivos Thin client.



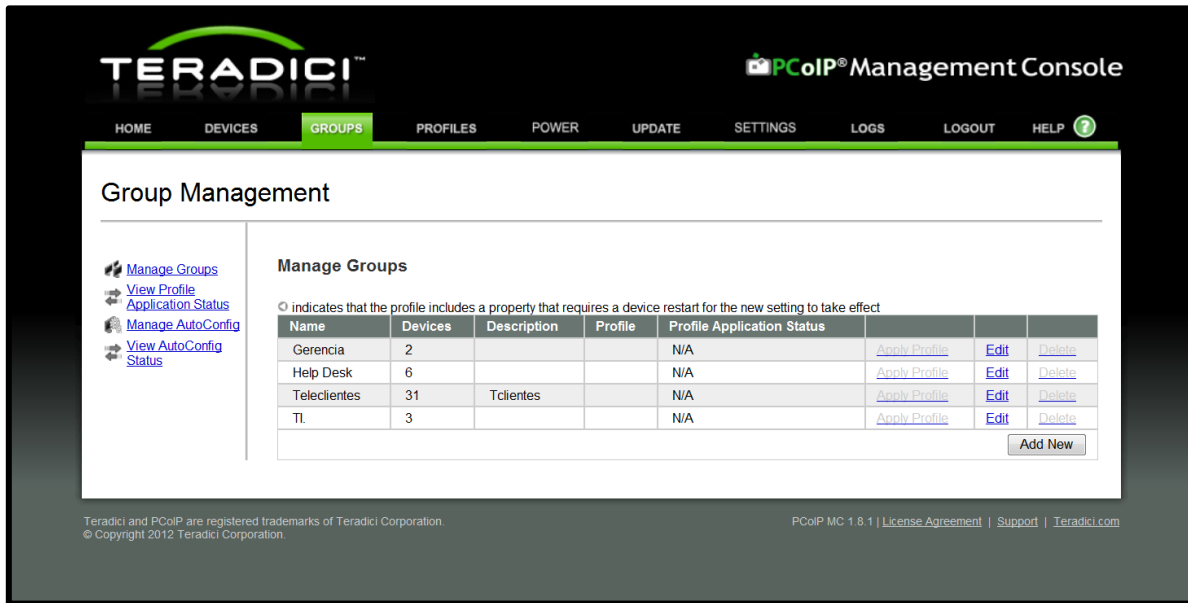
Fuente: <https://teradici.corp>

- Agregando los dispositivos de a grupos:

Una vez rastreados los dispositivos instalados, la practicante creo y agregó nuevos grupos de acuerdo al área donde fueron instaladas las thin client, tal y como se muestra en la gráfica 36 y después cada dispositivo era asignado a un grupo para una mejor administración a la hora de realizar una nueva actualización o configuración tal y como se observa en la gráfica 37.

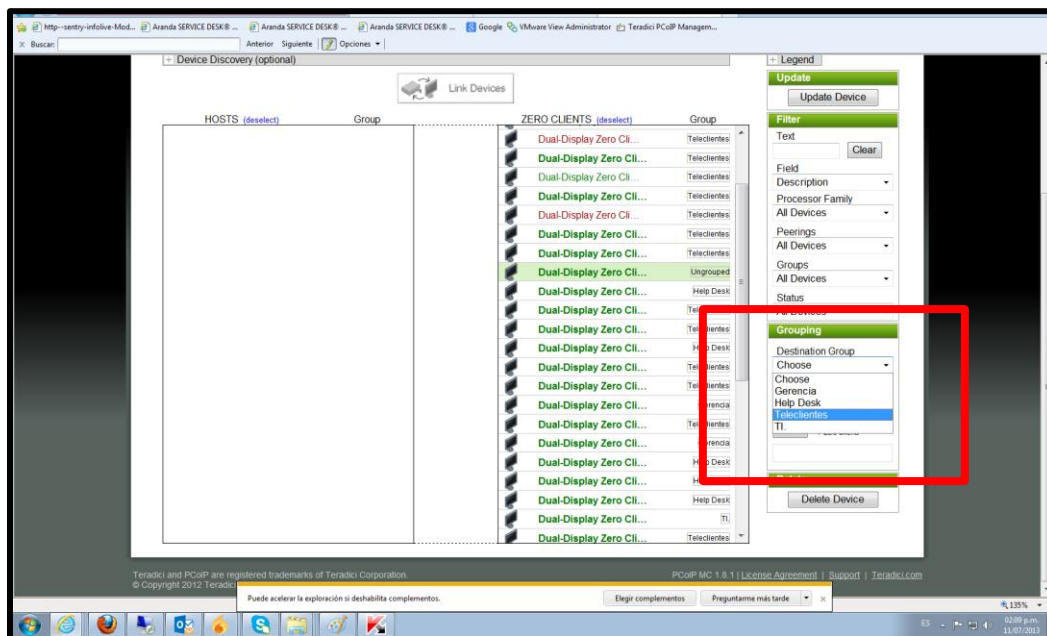


GRÁFICO 36. Agregar grupo nuevo.



Fuente: <https://teradici.corp>

GRÁFICO 37. Asignación de maquina a un grupo.



Fuente: <https://teradici.corp>

- Programando actualizaciones de firmware, aplicaciones de perfil y energía:

El **firmware** es un bloque de instrucciones de máquina para propósitos específicos, grabado en una memoria, normalmente de lectura / escritura que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. En resumen, un firmware es el software que maneja al hardware.

Dicho esto, desde la consola de administración teradici se ejecutó durante el periodo de práctica 2 actualizaciones del firmware. Para esto la practicante se registró en la página [www.teradici.com](http://www.teradici.com) para descargar las actualizaciones PCoIP en <http://techsupport.teradici.com/ics/support/DLSplash.asp?task=download> consiguiendo una primera actualización del firmware con la versión 4.0.2, la cual fue configurada a todos los dispositivos con esta herramienta de administración tal y como se observa en el grafico 39 Y después una segunda actualización que saco teradici a los 3 meses con la versión 4.1.0 (Grafico 38).

### GRÁFICO 38. Actualización Firmware.

**Update Firmware**

[Import Firmware](#)  
[Update Devices](#)  
[View Status](#)

**Imported Firmware Files**

An imported firmware file can be deleted from the Management Console when there are no devices scheduled to be updated with the firmware file.

Device Family	Version	Description	Imported	Filename	Devices Scheduled		
Tera1	4.1.0	firmware 4.1.0 tera1	2013-06-26 15:00:10 COT	tera1_rel4-1-0_r4_1@14079.all	0	<a href="#">Update devices</a>	<a href="#">Delete</a>
Tera1	4.0.2	firmware 4.0.2 para tera1	2013-06-26 14:59:34 COT	tera1_rel4-0-2_rc_tera_r4_0_2@13079.all	0	<a href="#">Update devices</a>	<a href="#">Delete</a>

Refresh

Teradici and PCoIP are registered trademarks of Teradici Corporation.  
 © Copyright 2012 Teradici Corporation.

PCoIP MC 1.8.1 | [License Agreement](#) | [Support](#) | [Teradici.com](#)

Fuente: <https://teradici.corp>

**GRÁFICO 39. Versión firmware 4.0.2.**

**Selected Firmware Version**

Filename: **tera1\_rel4-1-0\_r4\_1@14079.all**

Device Family: **Tera1**

Version: **4.0.2**

File Description: **firmware 4.1.0 tera1**

**Begin updating targets at:**  
Updates scheduled in the past will begin immediately.

2013-07-11 14:40

**Device restart options:**

☒ Immediately restart Zero Clients when update is complete

☐ Schedule deferred restart on hosts when update is complete

[Select All](#) [Deselect All](#) [Schedule Update](#) [Cancel](#)

Select	Name	Type	Group	IP Address	Version	Device Family
<input checked="" type="checkbox"/>	pcoip-portal-0080648f34cf	Zero Client	TL		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080648f4365	Zero Client	Telecientes		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080643f3a50	Zero Client	Help Desk		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080648f4223	Zero Client	Telecientes		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080648f3e4f	Zero Client	Telecientes		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080648f3c3a	Zero Client	Telecientes		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080648f436b	Zero Client	Telecientes		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080643f1f8f	Zero Client	Telecientes		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080648f3f7a	Zero Client	Telecientes		4.0.2	Tera1
<input checked="" type="checkbox"/>	pcoip-portal-0080643f29e0	Zero Client	Telecientes		4.0.2	Tera1

Fuente: <https://teradici.corp>

## 9. CONCLUSIONES

La actualización constante del plan de contingencia es importante en una empresa, puesto que sirve como garantía y respaldo, si en un momento dado la información se encuentra en riesgo, sabiendo que va haber una documentación en la que se explica cómo recuperar la información, permitiendo a la empresa seguir en su cauce, sin que los usuarios finales se vean afectados.

Para la contingencia en una empresa también es de suma relevancia, estar pendiente del estado de la ejecución de los backup y mantener una documentación de estos debido a que forman parte del respaldo a la pérdida de datos o daños inesperados, además de que en cualquier momento puede haber una auditoria externa donde todo debe estar en orden por el bien y salud de la empresa.

En la implementación del software Aranda Metrix, se vieron buenos resultados ya que este software es de gran ayuda para el cumplimiento de las normas administrativas en cuanto a la reducción de software no licenciado al interior de la empresa y como ejemplo de esto, Microsoft realizo una auditoria en este semestre en cuanto a su licenciamiento y fue todo un éxito.

La virtualización es una herramienta de ultima tecnología que trajo a la empresa múltiples ventajas; el aprovechamiento de recursos al poner varias máquinas en un solo equipo físico, ocupando menos espacio , reduciendo costos y haciendo provecho de las características del sistema, realizar modificaciones con las maquinas en ejecución sin ser percibido por los usuarios finales, reducir el costo de energía convirtiéndose en algo ecológicamente efectivo, el ahorro en el costo del mantenimiento de los equipos terminales, eficiencia al tener una menor cantidad de recursos para administrar, anchos de banda estandarizados, eficacia al no tener que parar las funciones laborales para realizar mantenimiento a las máquinas, mejor operación ya que la administración de todas las máquinas se hace de forma centralizada.

Por otra parte, hubo dificultades, debido a que, el plan de práctica basado en el plan de contingencia, no se logró llevar a cabalidad, pues la falta de tiempo y diversos compromisos por parte de trabajadores indispensables a la hora de conducir la práctica era limitada.

Para terminar, se puede concluir que la experiencia obtenida a partir de la práctica realizada, cumplió con la expectativa al tener una visión más cercana al área de sistemas y todas las funciones que esta cumple, puesto que, la nueva tecnología en la empresa “virtualización de escritorios” y las demás labores realizadas, hicieron que el aprendizaje fuera mucho más completo, retroalimentador y agradable.

## **10.RECOMENDACIONES**

Durante la experiencia, se logra denotar que el departamento de prácticas académicas, se debe asegurar de que las labores que el estudiante realizara al interior de la empresa a la cual se le ha vinculado, sean correspondientes con la carrera estudiada, para que de esta manera, se logre cumplir con las expectativas tanto de la empresa, la universidad y el estudiante, dado que, las vivencias obtenidas a partir de la practica en la primera empresa a la cual fui vinculada, no cumplió con las expectativas de aprendizaje practico relacionado con la carrera estudiada “Ingeniería en Sistemas y Telecomunicaciones”.

A su vez, a la empresa, se le recomienda brindar más tiempo de apoyo al estudiante, para que la elaboración de sus proyectos de práctica, logren ser cumplidos a cabalidad y de esta manera no se presenten proyectos con objetivos sin terminar.

## 11. BIBLIOGRAFIA

Soluciones de seguridad global. *Planes de contingencia*. <http://www.seguridad-la.com/artic/segcorp/7209.htm>

Comisión nacional de prevención de riesgos y atención de emergencias. *Componentes del plan de contingencia*. <http://www.cne.go.cr/CEDO-CRID/pdf/spa/doc1071/doc1071-c.pdf>

Reyes, Fredy (2011). Indicadores para el Diagnostico de Madurez Informática. Guías de Clase del módulo de Gerencia de Sistemas Informáticos. Especialización de Gerencia Informática. Universidad EAN.

Plan de contingencia Informático. Delegación Miguel Hidalgo. México, D.F. Archivo PDF. 2005.

*Intranet de UNE-Telefonía de Pereira*. <http://www.etp.com.co/etp/intranet/>

*Página oficial productos Wyse* <http://www.wyse.com/solutions/applications/call-center>.

Teradici Corporation. (2013). *TERADICI*. Recuperado el 26 de 06 de 2013, de <http://www.teradici.com/pcoip-technology.php>

VMware, inc. (2013). *VMware*. Recuperado el 12 de 06 de 2013, de [www.vmware.com](http://www.vmware.com)